Raréfaction dans les suites b-multiplicatives

Alexandre Aksenov

UNIVERSITÉ DE GRENOBLE

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE

Spécialité : **Mathématiques**

Arrêté ministériel : 7 août 2006

Présentée par

Alexandre Aksenov

Thèse dirigée par **Jean-Louis Verger-Gaugry**

préparée au sein **Institut Fourier**
et de **l'Ecole Doctorale MSTII**

Raréfaction dans les suites b-multiplicatives.

Thèse soutenue publiquement le 16 janvier 2014 ,
devant le jury composé de :

M., Roland Bacher
Maître de Conférences, Université Joseph Fourier , Examinateur
M., Cyril Banderier
Chargé de recherche, Université Paris-Nord , Examinateur
M., Jean-Marc Deshouillers
Professeur Emerite, Institut de Mathématiques de Bordeaux , Rapporteur
M., Michel Rigo
Professeur, Université de Liège, Rapporteur
M., Jean-Louis Verger-Gaugry
Chargé de recherche, Université Joseph Fourier, Directeur de thèse
M., Laurent Vuillon
Professeur, Université de Savoie, Examinateur

Table des matières

Remerciements

Je voudrais remercier mes parents qui ont déménagé en France en pensant avant tout à moi, qui ont été à l'écoute et qui m'ont aidé dans d'innombrables problèmes techniques. Je dois également mentionner Alina que je n'ai pas beaucoup vu pendant la période de préparation de la thèse, mais je ne peux pas voir comment mon premier résultat verrait le jour sans elle. Sans faire partie de ma famille, elle a été comme une sœur.

Je dois remercier les chercheurs de l'Institut Fourier dont mon directeur Jean-Louis Verger-Gaugry, qui s'exprime parfois à la limite de mes connaissances en langue française, mais qui ma guidé à travers la paperasse et qui a porté sur mes résultats un jugement auquel je pouvais faire confiance. Surtout, il a fait confiance au milieu de la préparation de la thèse en ma capacité de produire de nouveaux résultats. J'espère que le travail qui suit ne trahit pas celle-ci.
Je remercie également Roland Bacher pour les discussions mathématiques et pour son intérêt tout au long de la préparation de la thèse.
Je remercie Mikhail Zaidenberg pour m'avoir recommandé à l'Institut Fourier en premier lieu, ainsi qu'Alexei Pantchishkine : ils ont tous les deux bien aidé pour former mon premier réseau de connaissances.

Mes collègues du Laboratoire Jean Kuntzmann (Fédérico, Burak et les autres) et de l'Institut Fourier méritent sûrement une mention pour l'esprit de solidarité, les expéditions à l'extérieur et les conversations informelles qui ont rendu le travail moins pénible.

Je remercie les échecs et le club de Grenoble pour un re-enseignement des valeurs de concentration, esprit concret, respect des autres.

Je remercie les processus géologiques pour la montagne et la mairie de Grenoble pour la barre fixe. Les quelques bonnes idées de ce texte, s'il y en a, sont dues à cet endroit.

Enfin, la musique a été aussi nécessaire que l'air ; je mentionne particulièrement le groupe russe Liube.

En pensant à Thibaut.

Introduction

Cette thèse concerne le problème de raréfaction dans les suites multiplicatives.

Les suites b-multiplicatives généralisent la suite de Thue-Morse (ou Prouhet-Thue-Morse)

$$t_n = (-1)^{\text{le nombre de chiffres un dans l'écriture binaire de } n}.$$

Elle possède diverses propriétés telles que : elle évite le motif *uvuvu* (c'est à dire, c'est une suite "overlap-free") et pour chaque couple d'entiers naturels m, k tels que $m > k$ on a

$$\sum_{n=0}^{2^m-1} t_n n^k = 0.$$

Ces propriétés et d'autres sont répertoriées dans le texte [1]. La suite de Thue-Morse est définie par un automate fini et est multiplicative en base 2. Rappelons la définition générale : une suite b-multiplicative (t_n) est une suite de nombres complexes telle que pour tous entiers $a \in \{0, 1, \ldots, b-1\}$, $k \in \{0, 1, 2, \ldots\}$ et $c \in \{0, 1, \ldots, b^k - 1\}$ on a

$$t_{ab^k+c} = t_{ab^k} \cdot t_c$$

et $t_0 = 1$. On dira qu'elle vérifie la *condition de finitude* si on a de plus $t_{cb^k} = t_c$ pour tous $c, k \in \mathbb{N}$. Une suite b-multiplicative qui vérifie la condition de finitude est déterminée par ses termes $(t_0, t_1, \ldots, t_{b-1})$. Si, de plus, elle ne prend qu'un ensemble fini de valeurs (ce qui sera le cas de tous les exemples du texte), elle est b-automatique : un automate fini qui encode la table de multiplication de cet ensemble peut la calculer. Dans le sens réciproque, si une suite t_n à valeurs complexes est b-multiplicative et b-automatique, elle est de la forme

$$t_n = \bar{t}_{[\frac{n}{b^h}]} \cdot t_{n-b^h[\frac{n}{b^h}]} \quad ([x] \text{ désignant la partie entière de } x)$$

avec une suite $(\bar{t}_n)$ b^R-multiplicative qui vérifie la condition de finitude, avec des constantes $R, h \in \mathbb{N}, R > 0$. La preuve de cet énoncé (dont on peut comparer la conclusion avec le théorème 0.0.5 ci-dessous) ce trouve dans l'Annexe 6.

Étant donnée une suite (t_n), sa contrepartie p-raréfiée (ou avec le *pas de raréfaction* p) est définie pour $p \in \mathbb{N}^*$ comme la suite extraite $(t_{pn})_n$. Si (t_n) est b-multiplicative et définie par un automate fini, la suite p-raréfiée sera aussi b-automatique, mais, en général, pas b^s-multiplicative pour aucun s. La propriété de b-automaticité garantit essentiellement l'existence d'une fréquence de chaque symbole dans la suite raréfiée, une condition suffisante étant le fait que l'automate est fortement connexe (cf [2], Theorem 8.4.7). Le résultat suivant est plus précis :

Théorème 0.0.1 (Theorem 2,3 de [11]). *Soit H un groupe séparé, soit $b \in \mathbb{N} \setminus \{0, 1\}$ et soit $t_n \in H^{\mathbb{N}}$ une suite définie par : si $\overline{c_l c_{l-1} \ldots c_0}$ est l'expression en base b de $n \in \mathbb{N}$ alors*

$$t_n = t_{c_0} t_{c_1} \ldots t_{c_l}. \tag{1}$$

Supposons aussi que $t_0 = e$. Dans ce cas, la suite (t_n) est uniformément distribuée dans l'adhérence G du sous-groupe engendré par $t_0, t_1, \ldots, t_{b-1}$ munie de sa mesure de Haar.

Soit m le plus grand diviseur de $(b-1)$ tel que

$$\forall u \in \{0, 1, \ldots, b-1\} \; D(t_u) = \exp\left(-\frac{2i\pi u}{m}\right)$$

définisse une représentation continue du groupe G. Soient $p > 1$ et $r \geqslant 0$ deux entiers. Alors la suite (t_{pn+r}) est uniformément distribuée dans G muni de sa mesure de Haar si et seulement si $p \wedge m = 1$.

J'étudie des résultats encore plus précis concernant les sommes de termes initiaux d'une suite p-raréfiée. La problématique de p-raréfaction peut se formuler ainsi :

Problème général. *Quelles sont les propriétés asymptotiques des sommes*

$$\tilde{S}(N) = \sum_{n<N} 1_{p|n} t_n, t_n = \prod_i t_{c_i} si\ n = \overline{c_l \dots c_0}\ en\ base\ q$$

(Paramètres : p (le pas de raréfaction), $q, t_0, \dots, t_{q-1}$) ?

Exemples de question : trouver $\alpha_1 = \inf\{\alpha \in \mathbb{R} | \tilde{S}(N) = O(N^\alpha)\}$ (l'exposant de raréfaction) ; décrire $Q \in \mathbb{N}_{\geqslant 2}$ et une fonction F continue sur $[0,1]$ tels que

$$\tilde{S}(N) - F\left(\left\{\log_Q N\right\}\right) N^{\alpha_1} = o(N^{\alpha_1});$$

éventuellement trouver $\alpha_2 = \inf\{\alpha \in \mathbb{R} | \tilde{S}(N) - F\left(\left\{\log_Q N\right\}\right) N^{\alpha_1} = O(N^\alpha)\}$ (le deuxième exposant de raréfaction), etc.

D'après le théorème cité précédemment, $\tilde{S}(N) = o(N)$. A.O.Gelfond montre dans [18] que $\alpha_1 \leqslant \frac{\log 3}{\log 4}$ si t_n est la suite de Thue-Morse.

D.J.Newman ([28]) a montré en 1969 le résultat suivant qui est le premier résultat sur la raréfaction :

Proposition 0.0.2 (Conjecture de Moser)**.** *Pour tout $N > 0$, on a :* $\sum_{\substack{n<N \\ 3|n}} t_n > 0.$

De plus, on a

$$K_1 N^{\frac{\log 3}{\log 4}} < \sum_{\substack{n<N \\ 3|n}} t_n < K_2 N^{\frac{\log 3}{\log 4}},$$

où K_1 et K_2 sont deux constantes positives explicites.

La structure de ces sommes a été décrite de façon plus précise par J.Coquet dans [6] sous la forme suivante :

Proposition 0.0.3. *Pour tout $N \in \mathbb{N}^*$ on a :*

$$\sum_{\substack{n<N \\ 3|n}} t_n = F(\{\log_4 N\}) N^{\frac{\log 3}{\log 4}} + \epsilon(N) \tag{2}$$

où $\{x\}$ désigne la partie fractionnaire de $x \in \mathbb{R}$, $|\epsilon(N)| \leqslant \frac{1}{3}$ (et peut donc être considéré comme un terme d'erreur), et F est une fonction continue nulle part dérivable. De plus,

$$\inf F = \frac{2\sqrt{3}}{3} \approx 1,1547,$$

et

$$\sup F = \frac{55}{3}\left(\frac{3}{65}\right)^{\log_4 3} \approx 1,6020.$$

Une approximation du graphique de la fonction F se trouve dans l'Annexe 1, Figure 3.2.

On généralise la Proposition 0.0.3 en remplaçant 3 par un nombre premier p plus grand, pour chercher une formule de type

$$\sum_{\substack{n<N \\ p|n}} t_n = F(\{\log_{2^s} N\}) N^{\alpha_p} + \epsilon(N), \tag{3}$$

où F est une unique fonction continue, $s = s(p)$ est le plus petit entier strictement positif tel que $2^s \equiv 1 \bmod p$, et $\epsilon(N)$ est un terme dont l'exposant de croissance est inférieur à α_p. Dans l'Annexe 1, Figure 3.4 le lecteur trouvera une approximation du graphique de la fonction F publié dans [20] qui correspond au cas $p = 5$. Les exposants de raréfaction ont été donnés par J.-M. Dumont ([15]) pour les cas où $s(p) = p - 1$ ou alors $s(p) = \frac{p-1}{2}$ avec $p \equiv 3 \bmod 4$. Une formule de type (3), plus précise, a été obtenue dans l'article [19]. On renvoie le lecteur aux articles [12, 13] pour l'étude des nombres premiers p, pour lesquels les sommes (3) sont positives à partir d'un certain rang.

Si le pas de raréfaction est composé, les résultats aussi précis n'ont été obtenus que pour les puissances de petits nombres premiers ([20]). Dans le cas général on a le résultat suivant :

Théorème 0.0.4 (Proposition 2 dans l'article [13])**.** *Soit q en entier impair et s l'ordre de l'élément 2 de $(\mathbb{Z}/q\mathbb{Z})^\times$. Soit $\mathbf{T}$ la matrice $q \times q$ de la forme*

$$\mathbf{T} = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & & & 0 \\ & 1 & 0 & & 0 \\ & (0) & \searrow & \ddots & \vdots \\ & & & 1 & 0 \end{pmatrix}$$

et

$$\mathbf{M} = \prod_{m=0}^{s-1} (\mathbf{I} - \mathbf{T}^{2^m}).$$

Soit $V^{(u)}$ la somme directe des sous-espaces de $\mathbb{C}^q$ qui correspondent aux valeurs propres de module strictement plus grand que 1 et $\mathbf{P}_u$ la projection orthogonale sur ce sous-espace. Soit $\mathbf{S}_q(n) = (S_{q,i}(n))_{i=0,1,\dots,q-1} \in \mathbb{C}^q$. Alors la fonction

$$\mathbf{F}(n) = \mathbf{P}_u \mathbf{S}_q(n)$$

peut être prolongée en une fonction continue $\mathbf{F} : \mathbb{R}_+ \to V^{(u)}$ qui vérifie

$$\mathbf{F}(2^s x) = \mathbf{M}\mathbf{F}(x) \text{ pour tout } x > 0.$$

De plus, on a :

$$\mathbf{S}_q(n) - \mathbf{F}(n) = \begin{cases} O(1) & \text{si } \mathbf{M} \text{ n'a pas de valeurs propres de module 1} \\ O(\log n) & \text{sinon.} \end{cases}$$

Dans le même article, on trouve un résultat de positivité de $\tilde{S}(N)$ pour un pas de raréfaction multiple de 3 et N assez grand, rendu explicite dans [32].

La raréfaction dans les suites (b-multiplicatives, vérifiant la propriété de finitude) autres que Thue-Morse a été étudiée avec beaucoup de détails. On peut citer l'article ([8], Proposition 5) de F.M.Dekking et l'article ([22]) de R.Hofer. Ce dernier étudie les "suites de Thue-Morse avec poids" définies par

$$t_n = (-1)^{\gamma_0 c_0 + \gamma_1 c_1 + \dots + \gamma_l c_l}$$

où $\gamma_i \in \{0, 1\}$ et $\overline{c_l c_{l-1} \dots c_0}$ est l'expression de $n \in \mathbb{N}$ en base 2, et montre l'équivalence suivante :

Théorème 0.0.5. *Une suite de Thue-Morse avec des poids admet une formule de type*

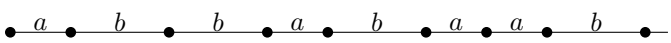
$$\sum_{\substack{n < N \\ n \equiv r \bmod 3}} t_n = F_r(\log_4 N) N^\alpha + \epsilon_r(N) \tag{4}$$

pour tout $r \in \{0, 1, 2\}$, où F_r sont des fonctions continues périodiques, $\alpha > 0$ et $\epsilon_r(N)$ sont des fonctions bornées, si et seulement si la suite γ_i est ultimement périodique.

La partie 1.1 de cette thèse généralise la partie directe du théorème 0.0.5 et le résultat de F.M.Dekking.

On peut remarquer que tous les énoncés précédents font intervenir une fonction continue, périodique et nulle part dérivable d'un argument réel. Ce phénomène est plus général, comme le montre l'article [34]. Le même auteur a étudié la distribution de la fonction à valeurs dans $\mathbb{Z}^r$ définie par $(s_q(h_1 n), \ldots, s_q(h_r n))$, où s_q désigne la somme des chiffres en base q d'un entier naturel, et $h_1, \ldots, h_r \in \mathbb{N}^*$ sont r pas de raréfaction différents.

Une motivation plus concrète pour l'étude des suites p-raréfiées vient des quasi-cristaux découverts en 1982. La suite de Thue-Morse peut définir un "quasi-cristal unidimensionnel" composé de segments de deux longueurs différentes a et b qui alternent suivant la suite de Thue-Morse :



La diffraction par un tel corps peut être modélisée comme le spectre de la mesure concentrée aux extrémités des segments. Différentes définitions de spectre existent ([21],[17]). Ce dernier texte ramène l'étude de la composante singulière continue du spectre à l'étude des sommes p-raréfiées de la suite de Thue-Morse.

Dans la partie 1.1 de cette thèse, on verra une expression similaire à (4) pour les sommes de premiers termes d'une large classe de suites b-multiplicatives :

Théorème 0.0.6. *Soit τ_n une suite b-multiplicative de nombres complexes de module inférieur ou égal à 1 qui vérifie la condition de finitude. On suppose aussi que $|\sum_{c=0}^{b-1} \tau_c| > 1$. Fixons une détermination L de $\log(\sum_{c=0}^{b-1} \tau_c)$. Alors, il existe une fonction continue $F : [0,1] \to \mathbb{C}$ qui dépend du choix de L telle que*

$$\sum_{n=0}^{N-1} \tau(n) = F\left(\{\log_b N\}\right) N^{\frac{L}{\log b}} \text{ pour tout } N \in \mathbb{N}^*. \tag{5}$$

La condition de finitude, la condition (1) et la condition formulée dans le Théorème 0.0.5 sont du même type. Dans la partie 1.2, on verra que le caractère autosimilaire des sommes de premiers termes, introduisant une fonction fractale, se généralise aux suites définies à partir d'un système de numération avec un ensemble de chiffres non standard (seront étudiés les ensembles de chiffres constitués de b nombres consécutifs, qui contiennent $-1, 0$ et 1).

Le phénomène de raréfaction dans une suite vérifiant la condition de finitude peut (en théorie) se décrire par la décomposition en p (où p est le pas de raréfaction) suites du même type ; ce sera l'objet de la partie 1.3. Cette méthode permet de décrire les propriétés asymptotiques des sommes raréfiées mais pas de répondre en général à la question étudiée dans l'article d'origine [28] et dans les textes plus récents [12, 13] : est-ce que les sommes p-raréfiées d'une suite b-multiplicative donnée gardent un signe constant à partir d'un certain rang ? On décrira dans la partie 1.4 une méthode due à Drmota et Skałba ([12]) pour donner une réponse négative à cette question dans le cas de la suite de Thue-Morse, et on décrira comment cette méthode peut être généralisée au cas plus général de suite b-multiplicative qui vérifie la condition de finitude et composée de nombres $1, 0$ et -1. La méthode générale dépend du signe du polynôme symétrique élémentaire de degré $p-2$ des nombres $\left(\sum_{c=0}^{b-1} t_c \zeta^{jc}\right)_{j=1,\ldots,p-1}$. On obtient des résultats intermédiaires (cf partie 2.5) de ce type par la méthode des *triangles de Pascal finis.*

La partie 1.3 et la partie 2 sont concentrées sur l'étude de l'exposant de croissance des sommes p-raréfiées associées aux suites composées de $+1, 0, -1$. D'après (5), pour une suite b-multiplicative (t_n) composée de

$+1, 0$ et -1, et vérifiant la condition de finitude, cet exposant vaut

$$\alpha_p = \frac{\log \left| \sum_{n=0}^{b^s-1} t_n \zeta^n \right|}{s \log b},$$

où les notations de la formule (3) sont reprises, $s = s(p)$ étant le plus petit entier strictement positif tel que $2^s \equiv 1 \bmod p$, et ζ une racine p-ième de l'unité telle que $|\sum_{n=0}^{2^s-1} t_n \zeta^n|$ soit maximal. Dans la partie 3 de [19] les auteurs étudient la valeur de $\xi := \sum_{n=0}^{2^s-1} t_n \zeta^n$ dans le cas où t_n est la suite de Thue-Morse (auquel cas $\zeta = 1$ ne correspond jamais au maximum de $|\xi|$), ζ est une racine primitive p-ième de l'unité et $s = p-1$ ou $s = \frac{p-1}{2}$. Dans le premier cas, $\xi = p$, et, dans le deuxième cas, ξ est décrit comme un entier du corps $\mathbb{Q}[\sqrt{(-1)^{\frac{p-1}{2}} p}]$. Dans le cas général, $\zeta = 1$ peut correspondre au maximum de $|\xi|$; les valeurs de ξ qui correspondent aux racines primitives de l'unité sont éléments d'un corps de nombres de degré au plus $\frac{p-1}{s}$, comme c'est montré dans la partie 2.3.

L'objet de la deuxième partie de cette thèse est le calcul de la norme de ξ au-dessus du corps des rationnels, c'est à dire du produit

$$\prod_{j \in \mathbb{F}_p^\times} \left(\sum_{c=0}^{b-1} t_c \zeta^{jc} \right) \tag{6}$$

(où $b \geqslant 2$ est la base de multiplicativité de la suite t_n, et $t_c \in \{-1, 0, +1\}$) et des autres polynômes symétriques élémentaires en $\left(\sum_{c=0}^{b-1} t_c \zeta^{jc}\right)_{j=1,\ldots,p-1}$. Pour cela on développe une méthode pour résoudre le problème suivant :

Problème 1. *Calculer le nombre de solutions d'une congruence linéaire*

$$f_1 x_1 + f_2 x_2 + \ldots + f_{p-1} x_{p-1} = 0 \tag{7}$$

dans $\mathbb{F}_p^{p-1}$, qui n'utilisent ni zéro ni deux fois un même élément de $\mathbb{F}_p^\times$, c'est à dire les nombres

$$\# \left\{ (x_1, \ldots, x_{p-1}) \in (\mathbb{F}_p^\times)^{p-1} \;\middle|\; \sum_{k=1}^{p-1} f_k x_k = 0,\ x_i \neq x_j \text{ si } i \neq j \right\}.$$

$\#\{\cdots\}$ désigne ici et par la suite la taille d'un ensemble.

On s'intéresse le plus souvent au nombre

$$\triangle_f = \frac{1}{\prod_{j \in \mathbb{F}_p} (\#\{k | f_k = j\})!} \left(\# \left\{ (x_1, \ldots, x_{p-1}) \in (\mathbb{F}_p^\times)^{p-1} \;\middle|\; \sum_{k=1}^{p-1} f_k x_k = 0,\ x_i \neq x_j \text{ si } i \neq j \right\} - \right.$$
$$\left. \# \left\{ (x_1, \ldots, x_{p-1}) \in (\mathbb{F}_p^\times)^{p-1} \;\middle|\; \sum_{k=1}^{p-1} f_k x_k = 1,\ x_i \neq x_j \text{ si } i \neq j \right\} \right),$$

qui suffit pour résoudre le Problème 1. Pour chaque p et pour chaque ensemble (qu'on peut supposer, sans perte de généralité, de la forme $\{0, a_1, a_2, \ldots, a_d\}$ où a_i sont distincts et non nuls) de valeurs des coefficients f_k, ces nombres forment un tableau, qu'on va appeler un *simplexe de Pascal fini*. Il s'agit d'une fonction

$$\mathbb{N}^d \supset \left\{ (n_{a_1}, n_{a_2}, \ldots, n_{a_d}) \middle| \sum n_{a_i} < p \right\} \to \mathbb{Z}$$

qui vérifie l'équation fonctionnelle de Pascal (cf les Théorèmes 2.3.2 et 2.4.3) dans tout le domaine sauf un petit (d'une taille qui sera appelée $F_0(\mathbf{a}, p)$ où $\mathbf{a} = (a_1, a_2, \ldots, a_d)$ dans la formule (2.61)) ensemble de points.

Remarquons que, d'après la même formule, $F_0(\mathbf{a}, p)$ ne dépend que des paramètres d et p, qui s'interprètent comme la dimension et la taille du simplexe.

Les normes (6), qui sont un cas particulier des polynômes symétriques, peuvent être calculées par une autre méthode plus rapide du point de vue calculatoire, en utilisant les résultants (cf la partie 3.1).

La partie 2.6 constitue une étude des simplexes de Pascal autres que ceux définis par la combinatoire modulo p. Son problème principal, la minimalité du nombre de points exceptionnels $F_0(\mathbf{a}, p)$ par rapport à tous les simplexes de Pascal finis, reste ouvert.

Chapitre 1

Raréfaction dans les suites b-multiplicatives

1.1 Sommes partielles de suites b-multiplicatives

Soit un entier $b > 1$, et soit (τ_n) une suite b-multiplicative telle que $\tau_{cb^k} = \tau_c$ et $|\tau(c)| \leqslant 1$ pour tous $c, k \in \mathbb{N}$. Par conséquent τ peut être définie de façon suivante : si $\overline{c_l c_{l-1} \dots c_0}$ est l'écriture d'un entier n en base b, alors

$$\tau_n = \prod_{i=0}^{l} \tau_{c_i}$$

et $\tau_0 = 1$; chacun des complexes $\tau_1, \tau_2, \dots, \tau_{b-1}$ est de module inférieur ou égal à 1. On supposera aussi que (τ_n) n'est pas constante.

Mettons la notation suivante : pour chaque $c \in \{0, \dots, b\}$, on notera $d(c) = \sum_{i=0}^{c-1} \tau_i$. Alors pour tout entier naturel non nul N écrit en base b comme $\overline{c_l c_{l-1} \dots c_0}$, on a :

$$\begin{aligned}
\sum_{n=0}^{N-1} \tau_n &= \sum_{n=0}^{\overline{c_l 00\dots0}-1} \tau_n + \sum_{n=\overline{c_l 00\dots0}}^{\overline{c_l c_{l-1} 0\dots0}-1} \tau_n + \dots + \sum_{n=\overline{c_l c_{l-1}\dots c_1 0}}^{N-1} \tau_n \\
&= \left(\sum_{c=0}^{c_l-1} \tau_c\right)\left(\sum_{c=0}^{b-1} \tau_c\right)^l + \tau_{c_l}\left(\sum_{c=0}^{c_{l-1}-1} \tau_c\right)\left(\sum_{c=0}^{b-1} \tau_c\right)^{l-1} + \dots + \prod_{k=1}^{l} \tau_{c_k} \cdot \left(\sum_{c=0}^{c_0-1} \tau_c\right) \qquad (1.1) \\
&= \sum_{i=0}^{l} \prod_{k=i+1}^{l} \tau_{c_k} \cdot d(c_i) \cdot d(b)^i.
\end{aligned}$$

On peut maintenant faire la distinction suivante en fonction du module de $d(b) = \sum_{c=0}^{b-1} \tau_c$.

Théorème 1.1.1. *Si $|\sum_{c=0}^{b-1} \tau_c| < 1$, la somme $\sum_{n=0}^{N-1} \tau_n$ est bornée.*

Si $|\sum_{c=0}^{b-1} \tau_c| = 1$, on obtient $\sum_{n=0}^{N-1} \tau_n = O(\log N)$.

Si $|\sum_{c=0}^{b-1} \tau_c| > 1$, alors pour toute valeur L du logarithme de $(\sum_{c=0}^{b-1} \tau_c)$, il existe une unique fonction continue $F : [0,1] \to \mathbb{C}$ telle que

$$\sum_{n=0}^{N-1} \tau(n) = F\left(\{\log_b N\}\right) N^{\frac{L}{\log b}} \text{ for all } N \in \mathbb{N}. \qquad (1.2)$$

Démonstration. Les deux premiers énoncés se déduisent directement de la formule (1.1), concentrons-nous donc sur le troisième. Remarquons que dans ce cas la dernière expression dans (1.1) a un sens pour tout réel positif.

Définition 1. *Étant donné $x \in \mathbb{R}_+^*$ écrit en base b comme $\overline{c_l c_{l-1} \dots c_0 . c_{-1} c_{-2} \dots}$, définissons $\psi(x) = \psi_{\tau,b}(x)$ par*

$$\psi(x) = \sum_{i=-\infty}^{l} \prod_{k=i+1}^{l} \tau_{c_k} \cdot d(c_i) \cdot d(b)^i. \qquad (1.3)$$

Cette définition doit être justifiée.

Lemme 1.1.2. *Soit x un nombre de la forme $x = b^{-m}X$, où $m, X \in \mathbb{N}$. Alors, l'expression (1.3) prend la même valeur pour les deux écritures de x en base b.*

Démonstration. Supposons que l'écriture de longueur finie de x est $\overline{c_l c_{l-1} \dots c_0 . c_{-1} c_{-2} \dots c_{-m}}$, et celle de longueur infinie est $c_l c_{l-1} \dots c_0 . c_{-1} c_{-2} \dots (c_{-m}-1)(b-1)(b-1)\dots$; le lemme équivaut alors à l'identité

$$\sum_{i=-m}^{l} \prod_{k>i} \tau_{c_k} \cdot d(c_i) d(b)^i = \sum_{i=-m+1}^{l} \prod_{k>i} \tau_{c_k} \cdot d(c_i) d(b)^i + \prod_{k>-m} \tau_{c_k} \cdot d(c_{-m}-1) d(b)^{-m} + d(b-1) \left(\sum_{i=-\infty}^{-m-1} \prod_{k>i} \tau_{c_k} \cdot d(b)^i \right).$$

Après la simplification des termes qui correspondent à $i > -m$, on obtient :

$$\prod_{k>-m} \tau_{c_k} \cdot d(c_{-m}) d(b)^{-m} = \prod_{k>-m} \tau_{c_k} \cdot d(c_{-m}-1) d(b)^{-m} + d(b-1) \left(\sum_{i=-\infty}^{-m-1} \prod_{k>i} \tau_{c_k} \cdot d(b)^i \right).$$

Après la soustraction du premier terme de la somme de droite, on obtient :

$$\prod_{k\geqslant -m} \tau_{c_k} \cdot d(c_{-m}) d(b)^{-m} = d(b-1) \left(\sum_{i=-\infty}^{-m-1} \prod_{k>i} \tau_{c_k} \cdot d(b)^i \right).$$

La simplification des produits conduit à l'égalité suivante :

$$d(b)^{-m} = d(b-1) \left(\sum_{i=-\infty}^{-m-1} \prod_{k=i+1}^{-m-1} \tau_{b-1} \cdot d(b)^i \right),$$

qui se transforme par un changement d'indices en

$$1 = d(b-1) \sum_{i=-\infty}^{-1} \tau_{b-1}^{-i-1} d(b)^i.$$

Le côté droit de cette expression vaut

$$d(b-1) \sum_{i=1}^{+\infty} \tau_{b-1}^{i-1} d(b)^{-i} = \frac{d(b-1)}{d(b)} \sum_{i=1}^{+\infty} \left(\frac{\tau_{b-1}}{d(b)} \right)^{i-1} = \left(1 - \frac{\tau_{b-1}}{d(b)} \right) \sum_{i=1}^{+\infty} \left(\frac{\tau_{b-1}}{d(b)} \right)^{i-1} = 1.$$

□

Par la même méthode on obtient la proposition suivante

Lemme 1.1.3. *La fonction ψ est continue.*

Démonstration. Considérons une suite réelle $x_1, x_2, \dots, x_n, \dots$ qui converge vers $x > 0$. Supposons que $x_n > x$ pour tout n, ou alors $x_n < x$ pour tout n. On choisira une écriture de x en base b en fonction de cette alternative : si $x_n > x$, soit $\overline{c_l c_{l-1} \dots c_0 . c_{-1} c_{-2} \dots}$ l'écriture de x qui ne se termine pas par des $b-1$, et si $x_n < x$ soit $\overline{c_l c_{l-1} \dots c_0 . c_{-1} c_{-2} \dots}$ l'écriture qui ne se termine pas des zéros.

Dans les deux cas, pour tout $m > 0$, il existe un rang N tel que pour tout $n > N$, x et x_n ont m chiffres identiques après la virgule. Par conséquent,

$$\begin{aligned} |\psi(x) - \psi(x_n)| &= \left| \sum_{i=-\infty}^{m-1} \prod_{k>i} \tau_{c_k} \cdot d(c_i) d(b)^i - \sum_{i=-\infty}^{m-1} \prod_{k>i} \tau(\bar{c}_k) \cdot d(\bar{c}_i) d(b)^i \right| \\ &\leqslant 2 \max_{c \in \{0,\dots,b-1\}} \textstyle\sum_{i<-m} |d(b)|^i \xrightarrow[m\to\infty]{} 0, \end{aligned}$$

où $\bar{c}_i$ sont les chiffres de x_n. La suite $(\psi(x_n))$ converge donc vers $\psi(x)$. □

D'après sa définition, $\psi(bx) = d(b)\psi(x)$. On peut maintenant définir la fonction F qui vérifie la formule (1.2). Pour tout $x > 0$, posons

$$F(\log_b x) = \psi(x) x^{-\frac{L}{\log b}}. \tag{1.4}$$

C'est une fonction continue d'un argument réel. L est la valeur de logarithme de $d(b)$ choisie au départ, et tous les logarithmes écrits dans la formule (1.4) sont supposés être réels. Montrons que F est périodique de période 1, ce qui termine la preuve de la partie existence. En effet, si $y = \log_b x$, alors

$$F(y+1) = F(\log_b(bx)) = d(b)\psi(x) \cdot b^{-\frac{L}{\log b}} x^{-\frac{L}{\log b}} = \psi(x) x^{-\frac{L}{\log b}} = F(y).$$

L'unicité de F vient du fait que la formule (1.2) fixe la valeur de F en un sous-ensemble dense de $[0,1]$. □

Pour finir cette partie, formulons une simple condition, sous laquelle les fonctions ψ et F ne sont dérivables nulle part.

Proposition 1.1.4. *Supposons que pour tout $c \in \{0, \dots, b-1\}$, $|\tau_c| > \frac{|d(b)|}{b}$. Alors les fonctions ψ et F ne sont dérivables nulle part.*

Démonstration. Nous allons utiliser la caractérisation suivante de la dérivée : si f est une fonction dérivable en x et $f'(x) = c$, alors pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que pour tous $x_1, x_2 \in \mathbb{R}$ tels que $x - \delta < x_1 \leqslant x \leqslant x_2 < x + \delta$ et $x_1 < x_2$, on ait

$$c - \epsilon < \frac{f(x_2) - f(x_1)}{x_2 - x_1} < c + \epsilon.$$

Supposons que pour tout $c \in \{0, \dots, b-1\}$, on a $|\tau_c| \geqslant \tau > \frac{|d(b)|}{b}$. Soit x un réel positif, et $\overline{c_l \dots c_0 . c_{-1} c_{-2} \dots}$ son écriture qui ne se termine pas par des $b-1$. Soit J_n la suite d'indices strictement croissante telle que $c_{-J_n} < b-1$. Posons

$$x_n = \overline{c_l c_{l-1} \dots c_0 . c_{-1} c_{-2} \dots c_{-J_n}}$$

et

$$y_n = \overline{c_l c_{l-1} \dots c_0 . c_{-1} c_{-2} \dots (c_{-J_n} + 1)}.$$

Alors $y_n > x \geqslant x_n$, $\lim_{n\to\infty}(y_n - x_n) = 0$ et

$$\psi(y_n) - \psi(x_n) = \prod_{k > -J_n} \tau_{c_k} \cdot d(b)^{-J_n} \cdot \tau_{c_{-J_n+1}}.$$

Par conséquent,

$$|\psi(y_n) - \psi(x_n)| \geqslant \tau^{l+1} \left(\frac{|d(b)|}{\tau}\right)^{-J_n}, \text{ d'où}$$

$$\left|\frac{\psi(y_n) - \psi(x_n)}{y_n - x_n}\right| \geqslant \left(\frac{|d(b)|}{\tau b}\right)^{-J_n} \xrightarrow[n\to\infty]{} +\infty.$$

La suite $\left(\frac{\psi(y_n)-\psi(x_n)}{y_n - x_n}\right)$ ne peut donc converger vers aucun complexe, d'où la fonction ψ ne peut pas être dérivable en x.

La fonction F est alors nulle part dérivable, d'après l'expression suivante pour $\psi(x)$:

$$\psi(x) = F(\log_b x) x^{-\frac{L}{\log b}}.$$

□

Remarquons que ce formalisme traite de façon uniforme le cas où $d(b)$ est réel et le cas où c'est un complexe. Le premier cas est typique pour l'étude de la raréfaction dans une suite réelle. Dans le deuxième cas, la fonction ψ a un comportement global d'une spirale logarithmique et n'admet pas de signe constant pour les arguments assez grands. Mentionnons une classe de suites de ce type (cf [8]) qui a été étudiée dans la littérature : il s'agit des suites p-multiplicatives (où p est premier) qui commencent par $(1, -e^{\frac{2i\pi}{p}}, e^{\frac{4i\pi}{p}}, -e^{\frac{6i\pi}{p}}, \ldots, e^{\frac{-2i\pi}{p}}, \ldots)$.

Une question naturelle concerne la dimension de Hausdorff du graphe de la fonction ψ. En général, elle est bornée supérieurement par $\min(2, \frac{\log b}{\log |d(b)|})$, mais on n'a une réponse précise que dans les cas les plus simples comme celui de la suite 4-multiplicative τ qui commence par $(1, e^{\frac{5i\pi}{3}}, e^{\frac{i\pi}{3}}, 1, \ldots)$ qui détermine l'étude des sommes de Thue-Morse 3-raréfiés comme on verra en chapitre 1.3, et dont le graphe (le flocon de Koch) se trouve dans l'Annexe 1. Si on considère les cas plus complexes, on sait seulement (cf [16]) que ces graphes sont des cas particuliers d'une construction itérative de fractales qui mène à la dimension $\min(2, \frac{\log b}{\log |d(b)|})$ presque sûrement.

1.2 Le cas d'un ensemble de chiffres autre que standard

Au début de ce chapitre, on utilisera la notation $x = \overline{c_l c_{l-1} \dots c_0}_{(Numération)}$ pour désigner le fait que $\overline{c_l c_{l-1} \dots c_0}$ est l'écriture de l'entier x en système de numération *(Numération)*, et on arrêtera plus loin de préciser le système de numération dans les formules pour les alléger.

Il sera consacré à la généralisation des résultats de la partie 1.1 aux systèmes de numération utilisant comme chiffres b entiers successifs quelconques contenant 0 et 1, et aux suites analogues aux suites b-multiplicatives vérifiant la condition de finitude. Si on note le plus petit chiffre $s \in \{2-b, \dots, 0\}$, on obtient le système de numération $(-s, s+b-1)$ (notation d'après les valeurs absolues du petit et du plus grand chiffre) d'après l'Exemple 3.6.7 du livre [2]. Il possède les propriétés suivantes :

(1) Il est parfait, c'est à dire chaque entier relatif peut être représenté par une unique suite finie de chiffres qui ne commence pas par zéro, par ailleurs, on peut ajouter un nombre quelconque de zéros à gauche d'une écriture dans le système $(-s, s+b-1)$ sans changer l'entier qu'elle représente. Une preuve de cet énoncé se trouve dans Theorem 3.6.2 du livre cité ci-dessus. L'existence d'une représentation est également conséquence de l'exercice 4.1.19 de [23], et son unicité a été démontrée dans la communication [25].

(2) La numération au système $(-s, s+b-1)$ préserve l'ordre, c'est à dire un entier relatif x est supérieur à un entier relatif y si et seulement si l'écriture de x en système $(-s, s+b-1)$ est supérieure à celle de y au sens de l'ordre lexicographique (une fois la plus courte a été complétée par des zéros à gauche pour que les deux écritures soient de longueur égale).

En effet, d'après (1), et le fait que l'ordre sur les entiers et l'ordre lexicographique sont des ordres totaux, il suffit de vérifier un seul sens d'implication. Soient $x = \overline{c_l c_{l-1} \dots c_0}_{(-s,s+b-1)}$ et $y = \overline{d_l d_{l-1} \dots d_0}_{(-s,s+b-1)}$ les écritures de deux entiers ramenées à une longueur commune, et supposons que $c_l > d_l$. Alors :

$$x \geqslant \overline{c_l \underbrace{ss \dots s}_{l}}_{(-s,s+b-1)} = c_l b^l + s \sum_{i=0}^{l-1} b^i = c_l b^l + \frac{s(b^l-1)}{b-1},$$

$$y \leqslant \overline{d_l \underbrace{(b+s-1)(b+s-1)\dots(b+s-1)}_{l}}_{(-s,s+b-1)} = d_l b^l + (b+s-1)\sum_{i=0}^{l-1} b^i = c_l b^l + \frac{(b+s-1)(b^l-1)}{b-1},$$

$$x - y \geqslant (c_l - d_l)b^l - (b^l - 1) = (c_l - d_l - 1)b^l + 1 \geqslant 1.$$

Les systèmes de numération de base négative $-b$ (avec les chiffres $0, 1, \dots, b-1$) sont une notion voisine. Une écriture d'un nombre dans un tel système doit être interprétée comme : $\overline{c_l c_{l-1} \dots c_0}_{(-b)} = \sum_{i=0}^{l} c_i (-b)^i$. Ils ont été étudiés directement par les auteurs de [2] (section 3.7) et [23] (section 4.1).

Les systèmes de numération $(b(b-1), b-1)$ peuvent facilement être convertis en base $-b$ et vice versa, grâce au fait que les entiers entre $b(1-b)$ et $b-1$ sont exactement les nombres qui s'écrivent en base $-b$ en deux chiffres. Si $\overline{c_l c_{l-1} \dots c_0}_{(-b)}$ est l'écriture en base $-b$ d'un entier x, on peut poser $C_i = \overline{c_{2i+1} c_{2i}}_{(-b)} \in [b(1-b), b-1]$ et obtenir $x = \overline{C_{[\frac{l+1}{2}]} \dots C_0}_{(b(b-1),b-1)}$ dans le système de numération $(b(b-1), b-1)$. Par conséquent, les systèmes de numération en base négative vérifient aussi les propriétés (1) et (2) ci-dessus.

On appellera une suite (τ_n) $(-s, s+b-1)$-multiplicative et vérifiant la condition de finitude par rapport au système de numération si on a

$$\tau_n = \prod_{i=0}^{l} \tau_{c_i}$$

pour tout entier $n = \overline{c_l c_{l-1} \dots c_0}_{(-s,s+b-1)}$, et $\tau_0 = 1$. Un exemple est la suite définie par

$$b = 4, s = -2,\ \tau_1 = -j, \tau_{-2} = -j, \tau_{-1} = j^2$$

où $j = e^{\frac{2i\pi}{3}}$. Elle est liée à la suite "de Thue-Morse en base -2" définie par

$$t_n = (-1)^{\text{le nombre de 1 dans l'écriture de } n \text{ en base } -2}.$$

t_n est défini pour tout entier n, mais on considère que la suite commence par $(t_0, t_1, t_2, \dots)$. Sous cette convention, le début de la suite de Thue-Morse en base -2 est

$$1\bar{1}\bar{1}\bar{1}\bar{1}11\bar{1}\bar{1}\bar{1}\bar{1}11\bar{1}\bar{1}\bar{1}11\bar{1}\bar{1}\bar{1}\bar{1}11\bar{1}\bar{1}\dots \quad (\text{où } \bar{1} \text{ désigne } -1).$$

On a $\tau_n = t_n j^n$, ce qui suggère que cette suite peut être utilisée dans l'étude des sommes 3-rarefiées de (t_n). Le tracé des sommes initiales de la suite (τ_n) de cet exemple se trouve dans l'Annexe 1, Figures 3.5-3.7.

On établira une formule analogue au cas particulier où tous les chiffres sont positifs ou nuls. Notons $d(c) = \sum_{s \leqslant c' < c} \tau_{c'}$ pour chaque $c \in \{s, \dots, s+b\}$ et $d = d(s+b)$ la somme des valeurs de la suite aux chiffres du système de numération. Si un entier naturel N s'écrit comme $\overline{c_l c_{l-1} \dots c_0}$ au système de numération $(-s, s+b-1)$, alors

$$\begin{aligned}
\sum_{n=0}^{N-1} \tau_n &= \sum_{n=0}^{\overline{c_l ss\dots s}-1} \tau_n + \sum_{n=\overline{c_l ss\dots s}}^{\overline{c_l c_{l-1} s\dots s}-1} \tau_n + \dots + \sum_{n=\overline{c_l c_l - 1 \dots c_1 s}}^{N-1} \tau_n \\
&= \left(\sum_{c=0}^{c_l-1} \tau_c\right)\left(\sum_c \tau_c\right)^l + \tau_{c_l}\left(\sum_{c<c_{l-1}} \tau_c\right)\left(\sum_c \tau_c\right)^{l-1} + \dots + \textstyle\prod_{k=1}^{l} \tau_{c_k} \cdot \left(\sum_{c<c_0} \tau_c\right) \qquad (1.5) \\
&= \left(\textstyle\sum_{0 \leqslant c < c_l} \tau_c\right) d^l + \sum_{i=0}^{l-1} \prod_{k=i+1}^{l} \tau_{c_k} \cdot d(c_i) \cdot d^i
\end{aligned}$$

On supposera que $|d| > 1$. La formule (1.5) suggère une autosimilarité, mais celle-ci ne peut pas être décrite par le formalisme précédent. En fait, si on essaie d'appliquer (1.5) aux nombres réels, la nouvelle fonction ne coïncidera pas avec les sommes partielles de la suite (τ_n) aux points entiers car $d(0) \neq 0$.

On énoncera l'autosimilarité des sommes partielles de (τ_n) à l'aide de l'idée suivante : le segment qui correspond aux nombres de longueur $l+1$ est obtenu de celui qui correspond aux nombres de longueur l par une similarité de rapport d. Précisément on a la

Proposition 1.2.1. *Soit $N > 0$ un entier qui s'écrit au système de numération $(-s, s+b-1)$ comme $\overline{c_l c_{l-1} \dots c_0}$, et M un entier qui s'écrit comme $\overline{c'_{l'} c'_{l'-1} \dots c'_0}$. Supposons que*

$$\frac{N - \overline{1\underbrace{ss\dots s}_{l}}}{b^l} = \frac{M - \overline{1\underbrace{ss\dots s}_{l'}}}{b^{l'}}. \qquad (1.6)$$

Alors

$$\left(\sum_{n=\overline{1\underbrace{ss\dots s}_{l}}}^{N-1} \tau_n\right) d^{l'-l} = \sum_{n=\overline{1\underbrace{ss\dots s}_{l'}}}^{M-1} \tau_n. \qquad (1.7)$$

Démonstration. Supposons que $l' > l$. Alors, d'après (1.6), l'écriture de M est $\overline{c_l c_{l-1} \dots c_0 ss\dots s}$ avec $(l'-l)$

chiffres s et on a :

$$\sum_{n=\overline{1\underbrace{ss\dots s}_{l'}}}^{M-1}\tau_n = \sum_{n'=\overline{1\underbrace{ss\dots s}_{l}}}^{N-1}\ \sum_{n=\overline{(n')\underbrace{ss\dots s}_{l'-l}}}^{\overline{(n'+1)\underbrace{ss\dots s}_{l'-l}}-1}\tau_n \quad = \sum_{n'}\tau_{n'}\ \sum_{\bar{n}=\overline{\underbrace{ss\dots s}_{l'-l}}}^{\overline{\underbrace{(s+b-1)(s+b-1)\dots(s+b-1)}_{l'-l}}}\tau_{\bar{n}} = d^{l'-l}\sum\tau_{n'}.$$

Ici les écritures $\overline{(n')ss\dots s}$ et $\overline{(n'+1)ss\dots s}$ correspondent aux nombres dont l'écriture commence par celle de n' (ou $n'+1$) et continue par des s. □

Remarque. Dans cet énoncé, on peut associer au nombre $N = \overline{1\underbrace{ss\dots s}_{l+1}}$ (le plus petit entier naturel qui s'écrit avec $l+2$ chiffres) la longueur l. Le rapport (1.6) correspondant est

$$\frac{N - \overline{1\underbrace{ss\dots s}_{l}}}{b^l} = b+s-1,$$

qui est sa valeur maximale.

À l'aide de la Proposition 1.2.1 on pourra construire une fonction fractale qui prolonge la fonction somme des premières valeurs de τ. Introduisons pour celle-ci la notation

$$\tilde{\psi}(N) = \sum_{n=0}^{N-1}\tau_n\ (N\in\mathbb{N}).$$

À chaque $x \geqslant 1$ on associe sa *longueur* $l(x)$ définie par : $x \in \left[\overline{1\underbrace{ss\dots s}_{l}},\ \overline{1\underbrace{ss\dots s}_{l+1}}\right[$ et le réel

$$\alpha(x) = \frac{x - \overline{1\underbrace{ss\dots s}_{l}}}{b^l} \in [0, b+s-1[.$$

Notons pour tout $m\in\mathbb{N}$,

$$x_m = \overline{1\underbrace{ss\dots s}_{l+m}} + \left[b^{l+m}\alpha(x)\right]$$

puis

$$\frac{\psi(x) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l}})}{d^l} := \lim_{m\infty}\frac{\tilde{\psi}(x_m) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l+m}})}{d^{l+m}}. \tag{1.8}$$

Cette fonction vérifie les propriétés suivantes analogues à celles de la fonction ψ définie dans la preuve du Théorème 1.1.1 :

Théorème 1.2.2. *La fonction*

$$\psi :\ [1,+\infty[\to\mathbb{C}$$

est bien définie par la formule (1.8)*, continue, elle prolonge* $\tilde{\psi}$ *et vérifie pour tous* $x,y\in[1,+\infty[$ *tels que* $\alpha(x)=\alpha(y)$ *et* $l=l(x)=l(y)+1$ *l'équation*

$$\psi(x) - \psi(\overline{1\underbrace{ss\dots s}_{l}}) = d\cdot\left(\psi(y) - \psi(\overline{1\underbrace{ss\dots s}_{l-1}})\right). \tag{1.9}$$

Démonstration. La suite dans (1.8) converge car on peut borner la différence entre ses deux termes successifs. Soit $x \geqslant 1$ et $m \in \mathbb{N}$. On a alors, d'après la proposition 1.2.1 :

$$\frac{\tilde{\psi}(x_m) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l+m}})}{d^{l+m}} = \frac{\tilde{\psi}\left(\overline{1\underbrace{ss\dots s}_{l+m+1}} + b\left[b^{l+m}\alpha(x)\right]\right) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l+m+1}})}{d^{l+m+1}},$$

d'où

$$\frac{\tilde{\psi}(x_{m+1}) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l+m+1}})}{d^{l+m+1}} - \frac{\tilde{\psi}(x_m) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l+m}})}{d^{l+m}} = \frac{\tilde{\psi}(x_{m+1}) - \tilde{\psi}\left(\overline{1\underbrace{ss\dots s}_{l+m+1}} + b\left[b^{l+m}\alpha(x)\right]\right)}{d^{l+m+1}},$$

et

$$\left|\frac{\tilde{\psi}(x_{m+1}) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l+m+1}})}{d^{l+m+1}} - \frac{\tilde{\psi}(x_m) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l+m}})}{d^{l+m}}\right| < \frac{b}{d^{l+m+1}}.$$

Cette majoration montre que la suite du côté droit de (1.8) converge en effet, et on a

$$\left|\frac{\psi(x) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l}})}{d^{l}} - \frac{\tilde{\psi}(x_m) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l+m}})}{d^{l+m}}\right| < \frac{b}{(d-1)d^{l+m+1}}.$$

Si x est entier, alors pour chaque $m \in \mathbb{N}$, on a $x_m = \overline{1\underbrace{ss\dots s}_{l+m}} + b^{\,l+m}\alpha(x)$, et, d'après la Proposition 1.2.1, la suite utilisée pour définir $\psi(x)$ est stationnaire. Par conséquent $\psi(x) = \tilde{\psi}(x)$.

Pour montrer la continuité de ψ, nous allons distinguer deux situations : la continuité en un point autre que $\overline{1ss\dots s}$ et la continuité aux points qui restent. Si $x = 1$ ou $x > 1$ et x n'est pas de la forme $\overline{1ss\dots s}$, alors tout $\bar{x}$ assez proche x vérifie $l(\bar{x}) = l(x)$. Supposons que cette condition est remplie, ainsi que la condition $|x - \bar{x}| < \frac{1}{b^m}$ $(m \in \mathbb{N})$. On a alors $|x_m - \bar{x}_m| \leqslant 1$, d'où

$$\left|\frac{\psi(x) - \psi(\bar{x})}{d^l}\right| < \frac{1}{d^{l+m}} + \frac{2b}{(d-1)d^{l+m+1}}.$$

Par conséquent, la fonction ψ est continue en x.

Pour la continuité en un point $N = \overline{1\underbrace{ss\dots s}_{l}}$, on a besoin de la même manœvre que dans la preuve du lemme correspondant pour le Théorème 1.1.1 : distinguer deux expressions à priori différentes de $\psi(N)$. La continuité à droite en N se démontre par le raisonnement précédent. Pour traiter la continuité à gauche, considérons N comme un nombre de longueur $\bar{l}(N) = l - 1$. Un nombre $\bar{\psi}(N)$ sera défini de façon suivante analogue à $\psi(N)$: on a

$$\bar{\alpha}(N) = \frac{N - \overline{1\underbrace{ss\dots s}_{l-1}}}{b^{\,l-1}} = b + s - 1,$$

$$\overline{x_m}(N) = \overline{1\underbrace{ss\dots s}_{l+m}} = x_m(N) \text{ et}$$

$$\frac{\bar{\psi}(x) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l-1}})}{d^l} = \lim_{m\infty} \frac{\tilde{\psi}(x_m) - \tilde{\psi}(\overline{1\underbrace{ss\dots s}_{l+m-1}})}{d^{l+m-1}}. \tag{1.10}$$

Aux autres points, on considérera que $\bar{\psi} = \psi$. Le raisonnement précédent montre que la fonction $\bar{\psi}$ est continue à gauche. Or, d'après la remarque faite après la Proposition 1.2.1, on a aussi dans ce cas $\bar{\psi}(N) = \tilde{\psi}(N)$. La continuité de la fonction ψ est donc démontrée.

L'équation (1.9) vient du fait que, d'après ses hypothèses, on a pour tout $m \in \mathbb{N}^*$: $x_{m-1}(x) = x_m(y)$. □

On voit que les points $\psi(1), \psi(\overline{1s}), \psi(\overline{1ss})\dots$ sont des images l'un de l'autre par une similitude (du plan complexe) de rapport d. Un simple calcul montre que le centre de ces similitudes est le point $\omega = \frac{\psi(s+b)-d}{1-d}$. Dans l'exemple de la suite τ définie au début du chapitre, on a $d = 3e^{\frac{5i\pi}{3}}$ et $\omega = \frac{5+e^{\frac{4i\pi}{3}}}{7}$. Dans le cas de la section 1.1 (où $s = 0$), on a $\omega = 0$. L'affirmation ci-dessus, qui justifie la définition de ω, se formule de la façon suivante : pour tout $l \in \mathbb{N}$,

$$\psi(\overline{1\underbrace{ss\dots s}_{l}}) - \omega = d^l \left(\psi(1) - \omega\right).$$

La preuve par récurrence est facile.

Pour obtenir une formule analogue à (1.2), on a besoin d'une fonction analogue au logarithme ,et adaptée au système de numération $(-s, s+b-1)$. Ce rôle sera joué par

$$f(x) = \log_b \left(\frac{b-1}{b+s-1}(x-1) + 1\right).$$

Cette fonction (lisse et strictement croissante pour $x \geqslant 1$) vérifie : pour tout $l \in \mathbb{N}$ on a

$$f(\overline{1\underbrace{ss\dots s}_{l}}) = f\left(1 + \frac{(b+s-1)(b^l-1)}{b-1}\right) = l.$$

De plus, si deux réels x et y vérifient les hypothèses de l'équation (1.9), alors $f(x) = f(y) + 1$.

Cette correspondance avec les propriétés d'autosimilarité de la fonction ψ permet d'affirmer que pour tout $y \geqslant 0$ on a

$$\psi\left(f^{-1}(y+1)\right) - \omega = d\left(\psi\left(f^{-1}(y)\right) - \omega\right),$$

d'où la fonction F définie par

$$F(f(x)) = (\psi(x) - \omega)d^{-f(x)} \tag{1.11}$$

est périodique de période 1 et continue. Si on choisit une valeur L du logarithme de d, on peut mettre (1.11) sous une forme complètement analogue à (1.4) :

$$F(f(x)) = (\psi(x) - \omega)\left(\frac{b-1}{s+s-1}(x-1) + 1\right)^{\frac{L}{\log b}}. \tag{1.12}$$

Malgré le fait que ce formalisme est plus général que celui de la section 1.1, il utilise la même formule pour l'exposant de croissance de ψ. Quand on étudie ces exposants, on pourra considérer qu'on se trouve dans le cas où $s = 0$.

1.3 Sommes raréfiées des suites b-multiplicatives

Le phénomène de Newman peut être étudié en utilisant les résultats précédents. Supposons que (t_n) est une suite b-multiplicative qui vérifie la condition de finitude, p est un nombre premier et ζ est une racine primitive p-ième de l'unité. La somme p-raréfiée de (t_n) peut alors être exprimée sous la forme

$$\sum_{n<N} 1_{p|n} t_n = \sum_{n<N} \frac{1}{p}\left(1+\zeta^n+\zeta^{2n}+\ldots+\zeta^{(p-1)n}\right)t_n = \frac{1}{p}\left(\sum_{n<N} t_n + \sum_{n<N}\sum_{j\in\mathbb{F}_p^\times} \zeta^{jn} t_n\right).$$

Si on note s l'ordre de b dans le groupe $\mathbb{F}_p^\times$, on obtient que les suites $(\zeta^{jn}t_n)_n$ sont des suites b^s-multiplicatives.

La deuxième partie sera consacrée à l'étude de la constante $d(b^s)$ associée aux suites de la forme $\tau_n = \zeta^{jn}t_n$ où t_n est une suite de $+1, 0$ et -1. Mais avant de passer aux suites précises, ajoutons une remarque générale concernant les suites d'entiers raréfiées.

Considérons, comme précédemment, une suite b-multiplicative qui vérifie la condition de finitude et composée uniquement de nombres $-1, 0$ et 1. Soit p un nombre premier ne divisant pas b, considérons les mêmes nombres s, ζ et la suite τ, et le sous-groupe $< b >$ de $\mathbb{F}_p^\times$ engendré par b. Alors, la constante $d(b^s)$ associée à τ est

$$d(b^s) = \sum_{n=0}^{b^s-1} t_n \zeta^n,$$

par la b-multiplicativité de (t_n) elle peut aussi s'écrire comme

$$d(b^s) = \prod_{k=0}^{s-1}\left(\sum_{c=0}^{b-1} t_c \zeta^{b^k c}\right) = \prod_{j\in<b>}\left(\sum_{c=0}^{b-1} t_c \zeta^{jc}\right).$$

D'après cette formule, $d(b^s)$ est un nombre algébrique de degré au plus $\frac{p-1}{s}$. En effet, le groupe $\mathbb{F}_p^\times$ est composé de $\frac{p-1}{s}$ classes d'équivalence modulo $< b >$, et à chaque classe $[j]$ on associe le nombre

$$\xi^{[j]} = \sum_{n\,=\,0}^{b^s-1} t_n \zeta^{jn}.$$

Tous les polynômes symétriques en les $\xi^{[j]}$ sont des entiers, ce qui montre notre affirmation.

Étant donné ce résultat, il est naturel d'étudier les nombres

$$\xi^{[i]} = \prod_{j\in i\mathbb{F}_p^\times k} (\sum_{c=0}^{b-1} t_c \zeta^{jc})$$

(indépendamment de l'hypothèse $s = \frac{p-1}{k}$) au lieu des nombres $d(b^s)$, et ce point de vue sera adopté dans la partie 3.

A part la suite de Thue-Morse, on étudiera un autre exemple de suite b-multiplicative composée de $+1, 0$ et -1 qu'on va appeler la suite "$++-$". C'est la suite définie par

$$t_n = (-1)^{\text{le nombre de chiffres '2' dans l'écriture de } n \text{ en base } 3}. \tag{1.13}$$

Ses termes initiaux sont :

$$11\bar{1}\ 11\bar{1}\ \bar{1}\bar{1}1\ 11\bar{1}\ \ldots \quad (\text{où } \bar{1} \text{ désigne } -1).$$

1.4 Une méthode de traitement du phénomène de Newman pour les suites b-multiplicatives

Beaucoup de recherches sur la raréfaction dans la suite de Thue-Morse étaient motivées par le problème suivant :

Problème 2. *Soit (t_n) la suite de Thue-Morse. Pour quels nombres impairs p les sommes*

$$\sum_{n=0}^{N} t_{pn} \tag{1.14}$$

gardent-elles un signe constant pour N assez grand ?

Les auteurs des articles [28, 8, 20, 12, 13] ont exploré différentes classes de nombres p premiers. Dans les articles [8, 20, 13], la réponse est donnée pour certaines classes de nombres composés.

La partie 6 de [13] et l'article [14] introduisent une généralisation du Problème 2 qui doit être mentionnée. L'inégalité $\sum_{n=0}^{N} t_{pn} > 0$ équivaut à

$$\#\left\{n < N \;\middle|\; n \equiv 0 \bmod p \text{ et } s_2(n) \equiv 0 \bmod 2\right\} > \#\left\{n < N \;\middle|\; n \equiv 0 \bmod p \text{ et } s_2(n) \equiv 1 \bmod 2\right\},$$

où $s_2(n)$ est la somme des chiffres de n en base 2 (et, plus généralement $s_g(n)$ désignera la somme des chiffres de n en base g). Les auteurs des articles mentionnés étudient des classes de valeurs des paramètres (p, i, a, g, M) pour lesquelles on a, pour tout N assez grand :

$$\#\left\{n < N \;\middle|\; n \equiv i \bmod p \text{ et } s_g(n) \equiv M \bmod a\right\} = \max_m \#\left\{n < N \;\middle|\; n \equiv 0 \bmod p \text{ et } s_g(n) \equiv m \bmod a\right\}.$$

Nous allons généraliser le Problème 2 dans une direction différente en le considérant pour une suite b-multiplicative (t_n) qui vérifie la condition de finitude et est composée uniquement de nombres $-1, 0$ et $+1$, et pour p premier non divisant b. La description de la partie précédente exprime (1.14) comme une somme de p suites multiplicatives qui, individuellement, sont assez faciles à étudier, mais elle est mal adaptée à l'étude du signe de leur somme. Nous allons décrire dans un cadre général la méthode utilisée dans l'article [12] pour prouver le résultat négatif Theorem 1, puis à la fin du chapitre nous allons appliquer cette méthode à la suite "$++-$". La conclusion dépendra du problème assez délicat de signe de l'avant-dernier coefficient d'un polynôme annulateur évident d'un élément de $\mathbb{Q}(\zeta = e^{\frac{2i\pi}{p}})$. Les méthodes qui seront développées dans la deuxième partie de ce texte permettront d'y donner une réponse partielle. Nous allons supposer que b engendre multiplicativement le groupe $\mathbb{F}_p^\times$ (rappelons que, d'après la conjecture d'Artin, c'est le cas pour une infinité de premiers p). Nous allons chercher des contre-exemples au phénomène de Newman parmi les nombres $b^{p-1}, b^{p-2}, b^{p-3}, \ldots$ pour tout p assez grand et qui vérifie l'hypothèse ci-dessus.

Le formalisme qui sera introduit ci-dessous vaut en général et est compatible avec les notations de [12]. Sous les hypothèses de l'énoncé, la série génératrice de la suite t_n est de la forme

$$\prod_{j=0}^{M-1} \left(1 + t_1 x^{b^j} + t_2 x^{2b^j} + \ldots + t_{b-1} x^{(b-1)b^j}\right) = \sum_{n=0}^{b^M-1} t_n x^n$$

pour tout $M > 0$. Définissons ensuite les nombres $r_{M,k}^{(0)}$ par

$$\sum_{n=0}^{b^M-1} t_n x^n \equiv \sum_{k=0}^{p-1} r_{M,k}^{(0)} x^k \bmod x^p - 1.$$

Les entiers $r^{(0)}_{M,k}$ sont des sommes p-raréfiées de la suite (t_n) :

$$r^{(0)}_{M,k} = \sum_{\substack{n < b^M \\ n \equiv k \bmod p}} t_n.$$

Les nombres $r^{(0)}_{p-1,k}$ sont liés à l'exposant de raréfaction et sont relativement simples à déterminer pour une suite simple (notons le fait que $r^{(0)}_{p-1,k}$ sont tous égaux pour $k \neq 0$). Les nombres $r^{(0)}_{p-2,k}$ peuvent être déduits de la congruence polynomiale

$$\left(\sum_{k=0}^{p-1} r^{(0)}_{p-2,k} x^k\right)\left(1 + t_1 x^{\frac{1}{b}} + t_2 x^{\frac{2}{b}} + \ldots + t_{b-1} x^{\frac{b-1}{b}}\right) \equiv \sum_{k=0}^{p-1} r^{(0)}_{p-1,k} x^k \bmod x^p - 1 \tag{1.15}$$

(où les exposants de x sont des quotients dans le corps $\mathbb{F}_p$), et $r^{(0)}_{p-3,k}, r^{(0)}_{p-4,k}, \ldots$ peuvent être obtenus en appliquant successivement des formules similaires. Nous allons simplifier les expressions des exposants de x dans (1.15) en permutant les noms des nombres $r^{(0)}_{M,k}$ pour $k \neq 0$ (on considère qu'on peut se le permettre car les sommes raréfiées relatives aux restes non nuls modulo p ne font pas partie de l'objet d'étude). Posons

$$P^{(l)}_M(x) = \prod_{j=l}^{M-1} \left(1 + t_1 x^{b^j} + t_2 x^{2b^j} + \ldots + t_{b-1} x^{(b-1)b^j}\right)$$

pour tout couple d'entiers (M, l) tel que $0 \leqslant l < M$. Définissons les entiers $r^{(l)}_{M,k}$ par

$$P^{(l)}_M(x) \equiv \sum_{k=0}^{p-1} r^{(l)}_{M,k} x^k \bmod x^p - 1.$$

On a alors la relation $r^{(0)}_{p-1-l,k} = r^{(l)}_{p-1,b^l k}$, et les congruences suivantes analogues à (1.15) :

$$\left(\sum_{k=0}^{p-1} r^{(1)}_{p-1,k} x^k\right)\left(\sum_{c=0}^{b-1} t_c x^c\right) \equiv \sum_{k=0}^{p-1} r^{(0)}_{p-1,k} x^k \bmod x^p - 1, \tag{1.16}$$

$$\left(\sum_{k=0}^{p-1} r^{(2)}_{p-1,k} x^k\right)\left(\sum_{c=0}^{b-1} t_c x^{bc}\right) \equiv \sum_{k=0}^{p-1} r^{(1)}_{p-1,k} x^k \bmod x^p - 1 \text{ etc.} \tag{1.17}$$

Ces congruences se traduisent en systèmes d'équations linéaires circulants en variables $r^{(l+1)}_{p-1,k}$ et avec les nombres $r^{(l)}_{p-1,k}$ dans la partie de droite. Fixons la notation pour les matrices circulantes : on notera $C(a_0, a_1, \ldots, a_{p-1})$ la matrice

$$C(a_0, a_1, \ldots, a_{p-1}) = \begin{pmatrix} a_0 & a_{p-1} & a_{p-2} & \cdots & a_1 \\ a_1 & a_0 & a_{p-1} & \cdots & a_2 \\ a_2 & a_1 & a_0 & \cdots & a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{p-1} & a_{p-2} & a_{p-3} & \cdots & a_0 \end{pmatrix}.$$

Cette définition permet de transcrire la congruence (1.16) sous la forme

$$C(\theta_0, \theta_1, \theta_2, \ldots, \theta_{p-1}) \begin{pmatrix} r^{(1)}_{p-1,0} \\ r^{(1)}_{p-1,1} \\ \vdots \\ r^{(1)}_{p-1,p-1} \end{pmatrix} = \begin{pmatrix} r^{(0)}_{p-1,0} \\ r^{(0)}_{p-1,1} \\ \vdots \\ r^{(0)}_{p-1,p-1} \end{pmatrix}, \tag{1.18}$$

et la congruence (1.17) sous la forme

$$C(\theta_0, \theta_{\frac{1}{b}}, \theta_{\frac{2}{b}}, \ldots, \theta_{\frac{p-1}{b}}) \begin{pmatrix} r^{(2)}_{p-1,0} \\ r^{(2)}_{p-1,1} \\ \vdots \\ r^{(2)}_{p-1,p-1} \end{pmatrix} = \begin{pmatrix} r^{(1)}_{p-1,0} \\ r^{(1)}_{p-1,1} \\ \vdots \\ r^{(1)}_{p-1,p-1} \end{pmatrix}, \tag{1.19}$$

où les nombres en entrée des matrices sont définis par $\theta_c = \begin{cases} t_c & \text{si } c < b \\ 0 & \text{sinon} \end{cases}$, et les divisions dans les indices de la formule (1.19) sont des divisions dans $\mathbb{F}_p$.

Toutes les matrices circulantes se diagonalisent dans la base des vecteurs

$$\begin{pmatrix} 1 \\ \zeta^j \\ \zeta^{2j} \\ \vdots \\ \zeta^{-j} \end{pmatrix} (j \in \{0, 1, \ldots, p-1\}) \tag{1.20}$$

où ζ est une racine primitive p-ième de l'unité fixée, et la valeur propre correspondante pour une matrice $C(a_0, a_1, \ldots, a_{p-1})$ est

$$\sum_{i=0}^{p-1} a_i \zeta^{ij}. \tag{1.21}$$

Pour finir la description générale de la méthode, remarquons qu'on peut appliquer formellement le traitement matriciel même à une suite b-multiplicative quand b n'est pas un générateur du groupe $\mathbb{F}_p^\times$. Dans ce cas, les résultats seront vrais pour une autre suite qui est la suite b'-multiplicative (avec $b < b' < p$ et b' est un générateur de $\mathbb{F}_p^\times$) qui vérifie la condition de finitude et dont les b' premiers termes sont $\theta_0, \theta_1, \ldots, \theta_{b'-1}$.

Dans le cas où (t_n) est la suite de Thue-Morse (cf [12], Proposition 1), l'utilisation des vecteurs propres n'est pas obligatoire. Les auteurs obtiennent directement les résultats suivants :

$$r^{(0)}_{p-1,k} = \begin{cases} p-1 & \text{si } k = 0 \\ -1 & \text{sinon} \end{cases} \qquad \text{(comme conséquence du Corollaire 2.5.1)}\,; \tag{1.22}$$

$$r^{(1)}_{p-1,k} = \frac{p-1}{2} - k; \tag{1.23}$$

$$r^{(2)}_{p-1,0} = \frac{p-1}{2} - \frac{p^2-1}{24}. \tag{1.24}$$

Par conséquent, si $p > 11$ et 2 est un générateur du groupe $\mathbb{F}_p^\times$, les sommes p-raréfiées de la suite de Thue-Morse prennent des valeurs positives et négatives.

Dans le cas où (t_n) est la suite "$++-$", on n'a plus les mêmes expressions pour $r^{(l)}_{p-1,k}$. L'exposant de raréfaction (toujours sous l'hypothèse que 3 est un générateur modulo p) vaut

$$\alpha_p = \frac{\log L_p}{(p-1)\log 3}$$

où $L_p = \prod_{j=1}^{p-1}(1+\zeta^j-\zeta^{2j})$ (qui vaut le p-ième nombre de Lucas d'après le Théorème 2.5.2, mais on n'utilisera pas ce résultat dans cette section). On a ensuite

$$P^{(0)}_{p-1}(\zeta) = L_p = r^{(0)}_{p-1,0} - r^{(0)}_{p-1,1} \text{ , et}$$

$$P_{p-1}^{(0)}(1) = 1 = r_{p-1,0}^{(0)} + (p-1) r_{p-1,1}^{(0)}.$$

D'après ce système de deux équations,

$$\begin{cases} r_{p-1,0}^{(0)} = \dfrac{(p-1)L_p + 1}{p} \\ r_{p-1,1}^{(0)} = \dfrac{1 - L_p}{p} \end{cases}$$

Par conséquent, le vecteur $\left(r_{p-1,k}^{(0)}\right)_{k=0,\dots,p-1}$ se décompose en base des vecteurs propres (1.20) comme (remarquons que la formule suivante n'est rien d'autre que le calcul de sa transformée de Fourier discrète)

$$\begin{pmatrix} r_{p-1,0}^{(0)} \\ r_{p-1,1}^{(0)} \\ \vdots \\ r_{p-1,p-1}^{(0)} \end{pmatrix} = \begin{pmatrix} r_{p-1,0}^{(0)} \\ r_{p-1,1}^{(0)} \\ \vdots \\ r_{p-1,1}^{(0)} \end{pmatrix} = r_{p-1,1}^{(0)} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + L_p \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = r_{p-1,1}^{(0)} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + \frac{L_p}{p} \sum_{j=0}^{p-1} \begin{pmatrix} 1 \\ \zeta^j \\ \vdots \\ \zeta^{-j} \end{pmatrix}. \quad (1.25)$$

Comme la composante du vecteur $(1, 1, \dots, 1)$ vaut $r_{p-1,1}^{(0)} + \frac{L_p}{p} = \frac{1}{p}$, la décomposition du vecteur $\left(r_{p-1,k}^{(1)}\right)_{k=0,\dots,p-1}$ dans cette base est

$$\begin{pmatrix} r_{p-1,0}^{(1)} \\ r_{p-1,1}^{(1)} \\ \vdots \\ r_{p-1,p-1}^{(1)} \end{pmatrix} = \frac{1}{p} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + \sum_{j=1}^{p-1} \frac{L_p}{p(1 + \zeta^j - \zeta^{2j})} \begin{pmatrix} 1 \\ \zeta^j \\ \vdots \\ \zeta^{-j} \end{pmatrix}. \quad (1.26)$$

Par conséquent,

$$r_{p-1,0}^{(1)} = \frac{1}{p} + \frac{L_p}{p} \sum_{j=1}^{p-1} \frac{1}{1 + \zeta^j - \zeta^{2j}} = \frac{1}{p} + \frac{L_p}{p} \frac{\sigma_{p-2}(1 + \zeta - \zeta^2)}{\prod_\zeta (1 + \zeta - \zeta^2)} = \frac{1 + \sigma_{p-2}(1 + \zeta - \zeta^2)}{p}$$

où $\sigma_{p-2}(1+\zeta-\zeta^2)$ désigne le $(p-2)$-ième polynôme symétrique élémentaire en nombres de la forme $1+\zeta-\zeta^2$, ζ parcourant les racines p-ièmes primitives de l'unité. D'après Corollaire 2.5.5 (cf partie 2.5), on a : $r_{p-1,0}^{(1)} > 0$.

Nous sommes donc obligés de chercher un contre-exemple au phénomène de Newman plus loin. La décomposition du vecteur $\left(r_{p-1,k}^{(2)}\right)_{k=0,\dots,p-1}$ dans la base de vecteurs propres des matrices circulantes est la suivante :

$$\begin{pmatrix} r_{p-1,0}^{(2)} \\ r_{p-1,1}^{(2)} \\ \vdots \\ r_{p-1,p-1}^{(2)} \end{pmatrix} = \frac{1}{p} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} + \frac{L_p}{p} \sum_{j=1}^{p-1} \frac{1}{(1 + \zeta^j - \zeta^{2j})(1 + \zeta^{b'} - \zeta^{2b'})} \begin{pmatrix} 1 \\ \zeta^j \\ \vdots \\ \zeta^{-j} \end{pmatrix} \quad (1.27)$$

où le paramètre b' a été introduit pour couvrir le cas plus général où la suite à étudier est en fait une suite b'-multiplicative qui commence par $1, 1, -1, 0, 0, 0, \dots$ (cf la remarque qui suit la formule (1.21)). On en déduit :

$$p r_{p-1,0}^{(2)} = 1 + \frac{1}{L_p} \sigma_{p-2}\big((1 + \zeta - \zeta^2)(1 + \zeta^{b'} - \zeta^{2b'})\big).$$

Voici les premières valeurs de $\frac{1}{L_p}\sigma_{p-2}\big((1+\zeta-\zeta^2)(1+\zeta^{b'}-\zeta^{2b'})\big)$:

pour $p=5$: $\dfrac{1}{L_5}\sigma_{p-2}\big((1+\zeta-\zeta^2)(1+\zeta^3-\zeta)\big)=-1$;

pour $p=7$: $\dfrac{1}{L_7}\sigma_{p-2}\big((1+\zeta-\zeta^2)(1+\zeta^3-\zeta^6)\big)=-15$;

pour $p=11$: $\dfrac{1}{L_{11}}\sigma_{p-2}\big((1+\zeta-\zeta^2)(1+\zeta^6-\zeta^{12})\big)=-1$;

pour $p=13$: $\dfrac{1}{L_{13}}\sigma_{p-2}\big((1+\zeta-\zeta^2)(1+\zeta^6-\zeta^{12})\big)=-352$;

pour $p=17$: $\dfrac{1}{L_{17}}\sigma_{p-2}\big((1+\zeta-\zeta^2)(1+\zeta^3-\zeta^6)\big)=+2821$.

Chapitre 2

Étude de l'exposant de raréfaction

2.1 Revue des méthodes existantes

Cette partie sera consacrée à l'étude des nombres

$$\xi^{[a]} = \prod_{j \in a\Gamma} (\sum_{c=0}^{b-1} t_c \zeta^{cj}), \tag{2.1}$$

où ζ est une racine primitive p-ième de l'unité (avec p premier), Γ est un sous-groupe de $\mathbb{F}_p^\times$ et $t_c \in \{1, 0, -1\}$. Le cas qui correspond à une raréfaction dans la suite de Thue-Morse (c'est à dire celui où $b = 2$, $t_0 = 1$ et $t_1 = -1$) sous l'hypothèse $\Gamma =< 2 >$ a été étudié en détail dans la partie 3 de [19]. Rappelons les résultats de ce texte.

Le premier résultat est le suivant : pour toute suite (t_n), si le sous-groupe Γ est d'ordre pair, tous les nombres $\xi^{[a]}$ sont des réels positifs. En effet, on a $-1 \in \Gamma$ dans ce cas, donc le produit (2.1) est composé de paires de termes conjugués au sens complexe. Si Γ est d'ordre impair et (t_n) est la suite de Thue-Morse, alors

$$\prod_{j \in a\Gamma} (1 - \zeta^j) = \prod_{j \in \frac{1}{2}a\Gamma} (\zeta^{-j} - \zeta^j) = \prod_{j \in \frac{1}{2}a\Gamma} \left(2i \sin \frac{2\pi i}{p} \right),$$

où $\frac{1}{2}$ correspond à l'inverse de 2 dans $\mathbb{F}_p$. Donc, dans ce cas les nombres $\xi^{[a]}$ sont imaginaires purs (c'est une variante plus forte de la Proposition 3.3 de [19]).

Rappelons que $\xi^{[a]}$ sont des entiers algébriques de degré inférieur ou égal à $\frac{p-1}{|\Gamma|}$. Beaucoup de choses sont connues concernant ces nombres pour les petits degrés et la suite (t_n) de Thue-Morse. Par exemple, si $\Gamma = \mathbb{F}_p^\times$, alors $\xi^{[a]} = p$.

Si Γ est le sous-groupe des carrés dans $\mathbb{F}_p^\times$ et $p \equiv 3 \bmod 4$, on a (cf [19], partie 3 et [4]) :

$$\xi^{[1]} = (-1)^{\frac{h+1}{2}} i\sqrt{p}$$

où h est le nombre de classes d'idéaux du corps $\mathbb{Q}(\sqrt{-p})$, et $\xi^{[-1]} = -\xi^{[1]}$.

Si Γ est le sous-groupe des carrés, et $p \equiv 1 \bmod 4$, notons $\epsilon > 1$ l'unité fondamentale de l'anneau des entiers du corps $\mathbb{Q}(\sqrt{p})$, et h le nombre de classes d'idéaux de ce corps. Alors (cf Appendix de l'article [19] ainsi que [4]),

$$\xi^{[1]} = N_{\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{p})}(1 - \zeta) = \sqrt{p}\epsilon^h$$

et

$$\xi^{[i]} = \sqrt{p}\epsilon^{-h} \text{ si } i \text{ n'est pas un carré modulo } p.$$

On ne peut espérer obtenir des résultats analogues dans le cas d'une suite (t_n) quelconque qu'après avoir décrit les nombres $\xi^{[a]}$ qui correspondent au cas $\Gamma = \mathbb{F}_p^\times$. Décrivons tout de suite une méthode basée sur l'étude du résultant des polynômes $\tilde{P}(x) = t_0 + t_1 x + t_2 x^2 + \ldots + t_{d-1} x^{d-1} + t_b x^b$ et $x^p - 1$.

Supposons le polynôme $\tilde{P}$ irréductible et de degré d ; pour simplifier la description de la méthode, divisons-le par t_d. Notons le polynôme obtenu $P(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{d-1} x^{d-1} + x^d$. Alors

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(P(\zeta)) = \frac{1}{P(1)} \prod_{\zeta^p = 1} P(\zeta) = \frac{(-1)^d}{P(1)} \prod_{P(\phi)=0} (\phi^p - 1). \tag{2.2}$$

Exprimons les puissances de ϕ comme

$$\phi^n = x_0(n) + x_1(n)\phi + x_2(n)\phi^2 + \ldots + x_{d-1}\phi^{d-1},$$

où, pour tout $n \geqslant d-1$,

$$\begin{pmatrix} x_0(n+1) \\ x_1(n+1) \\ x_2(n+1) \\ \vdots \\ x_{d-1}(n+1) \end{pmatrix} = \begin{pmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & & & -c_1 \\ & 1 & 0 & & -c_2 \\ & (0) & \searrow & \ddots & \vdots \\ & & & 1 & -c_{d-1} \end{pmatrix} \begin{pmatrix} x_0(n) \\ x_1(n) \\ x_2(n) \\ \vdots \\ x_{d-1}(n) \end{pmatrix}. \tag{2.3}$$

Un calcul symbolique indépendant de p permet d'exprimer le dernier produit de (2.2) comme

$$\prod_{P(\phi)=0} (\phi^p - 1) = \mathbf{R}(x_0(p) - 1, x_1(p), \dots, x_{d-1}(p))$$

où $\mathbf{R} \in \mathbb{Z}[x_0, x_1, \dots, x_{d-1}]$ est un polynôme homogène de degré d.

La complexité de cette méthode dans le cadre où le polynôme P est fixe et p est variable correspond à celle du calcul de la puissance p-ième de la matrice compagnon, c'est à dire $O(p(\log p)^2)$.

Dans la suite de la deuxième partie de la thèse, nous développerons une méthode qui permet de calculer les valeurs de tous les polynômes symétriques en nombres $P(\zeta)$ où ζ parcourt les racines primitives p-ièmes de l'unité, donc de calculer un multiple du polynôme minimal de $P(\zeta)$. Sa complexité est celle de l'écriture d'un tableau de $O(p^d)$ entiers.

2.2 Combinatoire des partitions d'un ensemble

Dans cette section, nous allons résoudre le Problème 1 dans le cas particulier où tous les coefficients de l'équation linéaire valent 0 ou 1. Le résultat principal de la section est le suivant :

Lemme 2.2.1. *Soit p un nombre premier et $0 \leqslant n < p$ un entier. Notons $A_0(n,p)$ le nombre de sous-ensembles de $\mathbb{F}_p^\times$ de n éléments distincts de somme nulle (modulo p) et $A_1(n,p)$ le nombre de tels sous-ensembles dont la somme vaut 1. Alors*

$$A_0(n,p) - A_1(n,p) = (-1)^n.$$

Remarquons qu'un problème similaire a été résolu par V.S. Shevelev ([31]). Il y a deux différences entre son résultat et le Lemme 2.2.1 : d'une part V.Shevelev autorise les sous-ensembles qui contiennent zéro, d'autre part il autorise p à être premier ou composé.

Commençons la preuve par une remarque évidente : si on définit de façon analogue les nombres $A_2(n,p)$, $A_3(n,p)$, ..., $A_{p-1}(n,p)$, ils seront tous égaux à $A_1(n,p)$ car le produit d'un ensemble de somme 1 par une constante $c \in \mathbb{F}_p^\times$ est un ensemble de somme c, et cette correspondance entre sous-ensembles de $\mathbb{F}_p^\times$ est bijective.

Traitons une variante simplifiée du Lemme qui prend en compte l'ordre des éléments et autorise les répétitions, c'est à dire dénombre les objets suivants ;

Définition 2. *Notons $E_x^{k_1,k_2,\ldots,k_n}(n,p)$ (où $x \in \mathbb{F}_p$ et $k_1,k_2,\ldots,k_n \in \mathbb{F}_p^\times$) le nombre de suites $(x_1,x_2,\ldots,x_n)$ d'éléments de $\mathbb{F}_p^\times$ telles que*

$$\sum_{i=1}^{n} k_i x_i = x.$$

On notera aussi $E_x^{1,1,\ldots,1}(n,p)$ par $E_x(n,p)$.

On a alors la proposition suivante :

Proposition 2.2.2. *Si n est pair,*

$$E_0^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n + p - 1}{p} \quad \text{et} \quad E_1^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n - 1}{p};$$

si n est impair,

$$E_0^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n - p + 1}{p} \quad \text{et} \quad E_1^{k_1,k_2,\ldots,k_n}(n,p) = \frac{(p-1)^n + 1}{p}.$$

Dans les deux cas,

$$E_0^{k_1,k_2,\ldots,k_n}(n,p) - E_1^{k_1,k_2,\ldots,k_n}(n,p) = (-1)^n.$$

Démonstration. Par récurrence sur n. Si $n = 0$ ou $n = 1$ le resultat est trivial. Si $n \geqslant 2$ on a toujours :

$$E_0^{k_1,k_2,\ldots,k_n}(n,p) = (n-1)E_1^{k_1,k_2,\ldots,k_{n-1}}(n-1,p), \tag{2.4}$$

et

$$E_1^{k_1,k_2,\ldots,k_n}(n,p) = E_0^{k_1,k_2,\ldots,k_{n-1}}(n-1,p) + (p-2)E_1^{k_1,k_2,\ldots,k_{n-1}}(n-1,p), \tag{2.5}$$

car les suites de longueur n dont la combinaison linéaire vaut x sont exactement des prolongements des suites de longueur $n-1$ dont la combinaison linéaire est un autre résidu que x, et cette correspondance est bijective. On termine la récurrence en injectant les formules pour $n-1$ dans (2.4) et (2.5). □

Montrons maintenant le Lemme 2.2.1 pour les petites valeurs de n. Pour $n = 0$ ou $n = 1$ le Lemme est évident. Pour $n = 2$, il y a une suite $(x, y) \in \mathbb{F}_p^{\times 2}$ de somme nulle de plus, mais cela compte les suites répétitives de la forme (x, x). Comme p est premier, ces suites contribuent une fois pour chaque résidu non nul modulo p, et le fait de les écarter porte l'avantage de zéro à 2. On doit maintenant identifier chaque paire (x, y) avec (y, x), ce qui donne à nouveau une différence égale à un, et montre le Lemme 2.2.1 pour $n = 2$. Un calcul direct montre que $A_0(2, p) = \frac{p-1}{2}$ et $A_1(2, p) = \frac{p-3}{2}$.

Pour $n = 3$, le fait de compter toutes les suites $(x, y, z) \in \mathbb{F}_p^{\times 3}$ donne une différence $E_0 - E_1 = -1$. Parmi celles-ci, les suites (x, x, z) contribuent une fois de plus à la somme égale à 0, donc le fait de les écarter ajoute -1 à la différence globale. La même chose s'applique aux suites de la forme (x, y, y) et (x, y, x). Quand on l'a fait, on obtient une différence provisoire de -4, mais les triplets de la forme (x, x, x) ont été écartés 3 fois, ce qui équivaut à dire qu'ils comptent -2 fois. Ils doivent donc être "réinjectés" avec un coefficient 2. Comme p est premier et supérieur à 3, les triplets redondants contribuent une fois pour chaque résidu non-nul ; on accumule donc la différence de $-4 - 2 = -6$. On doit ensuite identifier les permutations c'est à dire diviser le score par 6, ce qui donne -1 comme résultat final.

Voici le calcul explicite pour le cas $n = 4$:

$$\begin{array}{ll}
1 & (\text{correspond à } E_0(4,p) - E_1(4,p)) \\
+6 & (\text{pour écarter } \begin{array}{lll} (x,x,y,z), & (x,y,x,z), & (x,y,z,x), \\ (x,y,y,z), & (x,y,z,y), & (x,y,z,z) \end{array}) \\
+2 \times 4 & (\text{pour réinjecter } (x,x,x,y), (x,x,y,x), (x,y,x,x) \text{ and } (x,y,y,y)) \\
+1 \times 3 & (\text{pour réinjecter } (x,x,y,y), (x,y,x,y) \text{ and } (x,y,y,x)) \\
+6 \times 1 & (\text{pour écarter } (x,x,x,x)) \\
= 24, &
\end{array}$$

ce qui vaut 4!, d'où le Lemme 2.2.1 est prouvé pour $n = 4$.

Pour n quelconque, on peut calculer la différence entre le nombre de suites de somme 0 et le nombres de celles de somme 1 avec un coefficient intermédiaire égal à 1 associé à chaque suite dans $\mathbb{F}_p^{\times n}$, puis réduire ce coefficient de 1 pour chaque paire de termes égaux, puis l'augmenter de 2 pour chaque triplet de termes égaux, puis procéder par ajustements successifs de coefficients ; chaque ajustement correspond à une "combinaison de poker" de n cartes. Si la somme des contributions de tous les ajustements et de $(-1)^n$ initial vaut $(-1)^n n!$, alors le lemme 2.2.1 est vrai pour n indépendamment de p à condition que $p > n$ soit premier.

Dans la suite, nous allons formaliser le concept de "combinaison de poker" en utilisant les notions exposées dans [24], et exposer le calcul décrit plus haut sous forme du principe d'inclusion-exclusion. Appelons une *partition* de l'ensemble $\{1, 2, \ldots, n\}$ un choix de sous-ensembles $B_1, B_2, \ldots, B_c$ de $\{1, 2, \ldots, n\}$ non-vides et deux-à-deux disjoints tels que $B_1 \cup B_2 \cup \cdots \cup B_c = \{1, 2, \ldots, n\}$ et la suite $(|B_i|)$ de leurs tailles est décroissante (on considère que la partition correspond à l'ensemble $\{B_1, B_2, \ldots, B_c\}$, et qu'une permutation des blocs B_i conforme à la condition précédente mène à une partition identique). L'ensemble Π_n des partitions de $\{1, 2, \ldots, n\}$ est partiellement ordonné par la relation suivante : étant données deux partitions τ et π, on dira que $\tau \geqslant \pi$ si chaque bloc de π est inclus dans un bloc de τ (c'est à dire si π est plus fine que τ). On définit la fonction de Möbius $\mu(\hat{0}, x)$ sur Π_n (cette définition et notation sont dues à [24]) récursivement par :
si $x = \{\{1\}, \{2\}, \cdots, \{n\}\} = \hat{0}$, alors $\mu(\hat{0}, x) = 1$;
si x est supérieur à $\hat{0}$, alors

$$\mu(\hat{0}, x) = - \sum_{\substack{y \in \Pi_n \\ y < x}} \mu(\hat{0}, y).$$

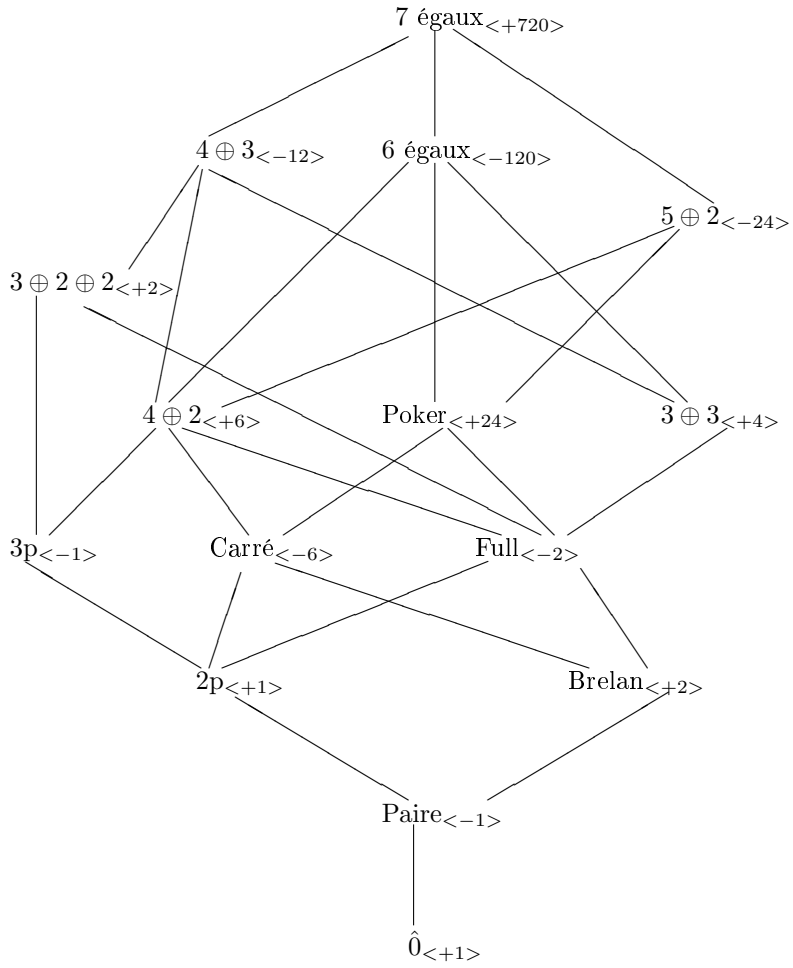


FIGURE 2.1 – Les partitions de 7 objets.

La Figure 2.1 montre la structure de Π_n dans le cas $n = 7$. Elle regroupe ensemble toutes les partitions de $\{1, 2, \ldots, 7\}$ de même *type* c'est à dire ayant une même suite $(|B_1|, |B_2|, \cdots, |B_n|)$ des tailles des blocs; les nombres entre parenthèses angulaires sont les valeurs de la fonction de Möbius associés à chaque type.

Cette figure utilise les noms suivants (empruntés au poker) pour les types des partitions :
- Paire : le type $(2, 1, 1, \ldots, 1)$.
- 2p, 3p : respectivement, la Double et la Triple paire c'est à dire les types $(2, 2, 1, 1, 1)$ et $(2, 2, 2, 1)$.
- Brelan : le type $(3, 1, 1, 1, 1)$
- Carré : le type $(4, 1, 1, 1)$.
- Poker : le type $(5, 1, 1)$.
- n égaux : le type $(n, 1, 1, \ldots, 1)$.
- Full : $(3, 2, 1, 1)$.
- $n_1 \oplus n_2 \oplus \ldots \oplus n_k$: le type $(n_1, n_2, \ldots, n_k, 1, 1 \ldots, 1)$.

D'après le corollaire de la Proposition 3, section 7 de [30] et le premier Theorem de la section 5.2.1 de [24], si x est une subdivision de type $(\lambda_1, \lambda_2, \cdots, \lambda_n)$, alors

$$\mu(\hat{0}, x) = \prod_{i=1}^{n} (-1)^{\lambda_i - 1} (\lambda_i - 1)!, \tag{2.6}$$

mais on n'aura bésoin de cette formule qu'à la section 2.3.

On utilisera aussi la définition suivante : soit $x = (x_1, x_2, \cdots, x_n)$ une suite de n résidus modulo p, vue

comme une fonction

$$x : \{1, 2, \cdots, n\} \to \mathbb{F}_p.$$

La *coimage* de x est alors la partition de $\{1, 2, \cdots, n\}$ composée des préimages non vides des éléments de $\mathbb{F}_p$. On peut maintenant montrer l'énoncé suivant qui met ensemble toute l'étude précédente.

Proposition 2.2.3. *La différence*

$$A_0(n, p) - A_1(n, p)$$

ne dépend pas de p à condition que p soit un nombre premier supérieur à n.

Démonstration. Nous décrirons un algorithme qui calcule cette différence (qui est exactement l'algorithme utilisé plus haut pour les petites valeurs de l'argument). Pour chaque subdivision $x \in \Pi_n$, notons $r_0(x, p)$ le nombre de suites $(x_1, x_2, \ldots, x_n)$ d'éléments de $\mathbb{F}_p^\times$ de coimage x et de somme 0, notons $r_1(x, p)$ le nombre de telles suites mais de somme 1, notons $r(x, p) = r_0(x, p) - r_1(x, p)$. Alors,

$$n!(A_0(n, p) - A_1(n, p)) = r(\hat{0}, p).$$

Notons, pour chaque subdivision y de $\{1, 2, \cdots, n\}$,

$$s(y, p) = \sum_{x \geqslant y} r(x, p).$$

Alors, par la Proposition 2.2.2,

$$s(y, p) = (-1)^{c(y)} \tag{2.7}$$

où $c(y)$ est le nombre de blocs dans la subdivision y. D'après la formule d'inversion de Möbius (cf [24]),

$$r(\hat{0}, p) = \sum_{y \in \Pi_n} \mu(\hat{0}, y) s(y, p) = \sum_{y \in \Pi_n} (-1)^{c(y)} \mu(\hat{0}, y). \tag{2.8}$$

En calculant cette somme, on obtient la valeur de $A_0(n, p) - A_1(n, p)$ de façon independante de p. □

Le dernier argument peut paraître artificiel [1], mais il suffit pour finir la démonstration du Lemme 2.2.1. Remarquons que $A_0(n, p) = A_0(n, p-1-n)$, car la somme d'un sous-ensemble de $\mathbb{F}_p^\times$ est nulle si et seulement si la somme de son complément est nulle. Pour la même raison, $A_1(n, p) = A_{-1}(n, p-1-n) = A_1(n, p-1-n)$.

On peut maintenant montrer le Lemme 2.2.1 par récurrence sur n. Il a déjà été vérifié pour les petites valeurs de n. Si $n > 4$, d'après le postulat de Bertrand il existe un nombre premier p' tel que $n < p' < 2n$. Remplaçons p par p' (cela mène à un énoncé équivalent d'après la Proposition 2.2.3) puis (en utilisant la remarque précédente) remplaçons n par $p' - 1 - n$. Comme $p' - 1 - n < n$, le pas de récurrence est achevé.

L'énoncé de départ, c'est à dire le calcul de $A_0(n, p)$, est une conséquence directe du Lemme 2.2.1. Voici le résultat :

Corollaire 2.2.4. *Soient $p, n \in \mathbb{N}$, p un nombre premier et $p > n$. Alors, si n est pair,*

$$A_0(n, p) = \frac{\binom{p-1}{n} + p - 1}{p}.$$

Si n est impair, on obtient

$$A_0(n, p) = \frac{\binom{p-1}{n} - p + 1}{p}.$$

1. Une preuve purement combinatoire et valable dans un cadre plus général existe : voir le chapitre 3, formule (31) de [33]

2.3 Les simplexes de Pascal

Nous allons chercher le nombre de solutions de la congruence (7) en le comparant avec le nombre de solutions de la congruence $f_1x_1 + f_2x_2 + \ldots + f_{p-1}x_{p-1} \equiv 1$, par analogie au cas particulier traité dans la section précédente. On supposera à partir de cette section que $p \geqslant 3$. Commençons par un groupe de définitions.

Définition 3. *Soit f une application linéaire de $\mathbb{F}_p^{p-1}$ dans $\mathbb{F}_p$ de la forme*

$$f(x_1, x_2, \ldots, x_{p-1}) = f_1x_1 + f_2x_2 + \ldots + f_{p-1}x_{p-1}. \tag{2.9}$$

Pour $j \in \mathbb{F}_p$, notons $N_j = N_j(f) = \big\{k \in \{1, \ldots, p-1\} \big| f_k = j\big\}$. Considérons l'action à gauche du groupe symétrique $\mathcal{S}_{p-1}$ sur $(\mathbb{F}_p^\times)^{p-1}$ et celle de ses sous-groupes $\mathcal{S}(N_j)$ (sous-groupes de toutes les permutations qui agissent par l'identité sur les éléments hors N_j). Notons alors pour chaque $i \in \mathbb{F}_p$:

$$B_i(f,p) := \#\left\{\sigma \in \mathcal{S}_{p-1} \;\middle|\; f(\sigma \cdot (1, \ldots, p-1)) = i\right\}, \tag{2.10}$$

$$C_i(f,p) := \#\left\{\sigma \in \mathcal{S}_{p-1}/\mathcal{S}(N_0) \;\middle|\; f(\sigma \cdot (1, \ldots, p-1)) = i\right\} \text{ et} \tag{2.11}$$

$$A_i(f,p) := \#\left\{\sigma \in \mathcal{S}_{p-1}/\mathcal{S}(N_0)\mathcal{S}(N_1)\ldots\mathcal{S}(N_{p-1}) \;\middle|\; f(\sigma \cdot (1, \ldots, p-1)) = i\right\}. \tag{2.12}$$

Notons $n_0(f)$ la taille de N_0, $n_1(f)$ la taille de N_1, etc.

Par exemple, si tous les coefficients de f sont des zéros ou des uns, alors

$$A_i(f,p) = A_i(n_1(f), p),\ C_i(f,p) = n_1(f)!A_i(n_1(f),p) \quad \text{et} \quad B_i(f,p) = n_0(f)!n_1(f)!A_i(n_1(f),p).$$

Dans tous les cas, les nombres A_i, B_i et C_i sont liés par

$$B_i(f,p) = n_0(f)!n_1(f)!\ldots n_{p-1}(f)!A_i(f,p) = n_0(f)!C_i(f,p). \tag{2.13}$$

Comme plus haut, les nombres $B_i(f,p)$ sont égaux pour tout $i \in \mathbb{F}_p^\times$. On notera

$$\triangle_f := A_0(f,p) - A_1(f,p).$$

Si la somme des coefficients de f est inférieure à p (ou, plus généralement, aucune somme d'un sous-ensemble des coefficients de f n'est multiple de p), la différence $\triangle_f$ se calcule comme dans la preuve du lemme 2.2.1, ce qui donne

$$\triangle_f = (-1)^{n_0(f)}\binom{n_1(f) + n_2(f) + \ldots + n_{p-1}(f)}{n_1(f), n_2(f), \ldots, n_{p-1(f)}} = (-1)^{n_0(f)}\frac{(n_1(f) + n_2(f) + \ldots + n_{p-1}(f))!}{n_1(f)!n_2(f)!\ldots n_{p-1}(f))!}. \tag{2.14}$$

Dans le cas contraire, la différence $\triangle_f$ n'est pas une fonction seulement de $n_1(f), n_2(f), \ldots$: une équation linéaire qui s'écrit de la même façon se comporte différemment pour différentes valeurs de p. Par exemple, si $f(x_1, x_2, \ldots) = 2x_1 + 3x_2$ et $p = 5$ alors

$$\triangle_f = -3,$$

et si $p = 7$ alors

$$\triangle_f = +2.$$

Des exemples de taille plus grande vont suivre.

Nous allons déterminer les nombres $\triangle_f$ en général par une approche globale, et dans ce chapitre nous allons prouver qu'ils vérifient la même équation que les coefficients multinomiaux (2.14).

Théorème 2.3.1 (L'équation de Pascal pour les coefficients coloriés)**.** *Soit p un nombre premier impair, et soit f une application linéaire de $\mathbb{F}_p^{p-1}$ dans $\mathbb{F}_p$ comme dans la définition 3. Supposons que les coefficients non nuls de f sont exactement $f_1, f_2, \ldots, f_n$, et $n \geqslant 1$. Soit alors, pour chaque $k \in \{1, \ldots, n\}$, $f \setminus [k]$ la forme linéaire qui est la même que f avec le k-ième coefficient remplacé par 0. On a la congruence suivante :*

$$C_0(f,p) - C_1(f,p) \equiv -\left(\sum_{k=1}^{n} (C_0(f \setminus [k], p) - C_1(f \setminus [k], p)\right) \mod p \tag{2.15}$$

et, si $\sum_{k=1}^{n} f_i \not\equiv 0$ mod p, on a l'égalité

$$C_0(f,p) - C_1(f,p) = -\left(\sum_{k=1}^{n} (C_0(f \setminus [k], p) - C_1(f \setminus [k], p))\right). \tag{2.16}$$

Démonstration. Appelons un *obstacle* une partie X de $\{1, \ldots, n\}$ telle que $\sum_{m \in X} f_m \equiv 0 \mod p$.

S'il n'y a aucun obstacle, alors d'après la preuve du lemme 2.2.1, on obtient

$$C_0(f,p) - C_1(f,p) = (-1)^n n!,$$

et ce nombre est l'opposé de n fois $(-1)^{n-1}(n-1)!$.

Dans le cas général, la formule (2.8) doit être remplacée par :

$$s(y,p) = (1-p)^{d(y)}(-1)^{c(y)} \tag{2.17}$$

si la partition y de $\{1, \ldots, n\}$ contient $d(y)$ obstacles parmi ses blocs. En effet, supposons que les blocs de y sont $B_1, \ldots, B_c$, et pour chaque bloc B_j on note $f_{B_j} = \sum_{m \in B_j} f_m \in \mathbb{F}_p$. Alors, choisir une solution de $f(x_1, \ldots, x_n, 0, \ldots, 0) = i$ telle que la coimage x de $(x_1, \ldots, x_n)$ vérifie $x \geqslant y$ (en tant que partitions) revient à choisir une solution $(x_{B_1}, \ldots, x_{B_c})$ de

$$\sum_{j=1}^{c} f_{B_j} x_{B_j} = i,$$

où les $x_{B_j} \in \mathbb{F}_p^\times$ ne sont plus obligés d'être différents. La Proposition 2.2.2 affirme que, si on ne prend pas en compte les indices j qui correspondent aux obstacles (c'est à dire ceux qui vérifient $f_{B_j} = 0$), la différence entre le nombre de solutions de $\sum_{j=1}^{c} f_{B_j} x_{B_j} = 0$ et de $\sum_{j=1}^{c} f_{B_j} x_{B_j} = 1$ vaut $(-1)^{c-d(y)}$. Le choix des valeurs de x_{B_j}, où B_j est un obstacle, est arbitraire (parmi $p-1$ possibilités pour chacun). Le produit de ces contributions mène à (2.17).

La formule (2.17) peut être écrite comme

$$s(y,p) = \sum_{l=0}^{d(y)} \sum_{\substack{X_1, X_2, \ldots, X_l \\ \text{obstacles contenus dans } y}} (-1)^{c(y)-l} p^l,$$

où la somme ne tient pas compte de l'ordre de $X_1, X_2, \ldots, X_l$. On obtient ensuite :

$$C_0(f,p) - C_1(f,p) = \sum_{y \in \Pi_n} \mu(\hat{0}, y) s(y,p) \tag{2.18}$$

$$= \sum_{\substack{X_1, X_2, \ldots, X_l \\ \text{obstacles disjoints}}} \sum_{\substack{y \in \Pi_n \\ y \text{ contient } X_1, \ldots, X_l \\ \text{parmi ses blocs}}} (-1)^{c(y)-l} \mu(\hat{0}, y) p^l \tag{2.19}$$

$$= \sum_{X_1, \ldots, X_l} \mu(\hat{0}, X_1)\mu(\hat{0}, X_2) \ldots \mu(\hat{0}, X_l) p^l$$

$$\times \sum_{\substack{y \in \Pi_n \\ y \text{ contient } X_1, \ldots, X_l}} \mu(\hat{0}, y - X_1 - X_2 - \ldots - X_l)(-1)^{c(y - X_1 - X_2 - \ldots - X_l)} \tag{2.20}$$

en factorisant $\mu(\hat{0}, y)$ d'après la formule (2.6). Dans la dernière somme, $(y - X_1 - X_2 - \ldots - X_l)$ désigne la partition y sans les blocs $X_1, \ldots, X_l$ (une partition de $(n - |X_1| - \ldots - |X_l|)$ éléments). Cette somme est égale à $(-1)^{n-|X_1|-\ldots-|X_l|}(n - |X_1| - \ldots - |X_l|)!$. Si $n > |X_1| + \ldots + |X_l|$, ce nombre est égal à l'opposé de la somme des termes correspondants pour toutes les formes $f \setminus [k]$ où $k \notin X_1 \cup \ldots \cup X_l$. En mettant ses remarques ensemble pour tous les ensembles $X_1, \ldots, X_l$ d'obstacles disjoints, on obtient la formule (2.16).

Quant à la congruence (2.15), notons que les termes de (2.20) qui proviennent des obstacles sont multiples de p, donc la congruence modulo p est valable même si l'ensemble $\{1, 2, \ldots, n\}$ lui-même est un obstacle.

□

Le nom de ce résultat reflète une intuition possible sous-adjacente à la définition des C_i : on colorie les coefficients de f en couleurs différentes, et on considère comme solutions différentes les permutations des x_i entre les positions associées à des coefficients égaux mais de couleur différente. Par exemple, si $p = 7$ et $f(x_1, x_2, x_3, x_4) = x_1 + 2x_2 + 2x_3 + 3x_4$, les solutions

$$(1 \text{ noir}) \cdot 4 + (2 \text{ rouge}) \cdot 1 + (2 \text{ vert}) \cdot 2 + (3 \text{ noir}) \cdot 6 = 0 \tag{2.21}$$

et

$$(1 \text{ noir}) \cdot 4 + (2 \text{ rouge}) \cdot 2 + (2 \text{ vert}) \cdot 1 + (3 \text{ noir}) \cdot 6 = 0 \tag{2.22}$$

sont considérées comme différentes. Notons que dans cet exemple, on peut facilement déduire l'identité $A_0(f) - A_1(f) = +5$ des trois suivantes :

$$\begin{aligned} A_0(x_1 + 2x_2 + 2x_3) - A_1(x_1 + 2x_2 + 2x_3) &= -3, \\ A_0(x_1 + 2x_2 + 3x_4) - A_1(x_1 + 2x_2 + 3x_4) &= -6, \\ A_0(2x_2 + 2x_3 + 3x_4) - A_1(2x_2 + 2x_3 + 3x_4) &= +4. \end{aligned}$$

La variante suivante du théorème intégré, dans un sens, cette subtilité dans la preuve.

Théorème 2.3.2 (L'équation de Pascal pour les coefficients non-coloriés)**.** *Soit p un nombre premier impair, et f une application linéaire de $\mathbb{F}_p^{p-1}$ dans $\mathbb{F}_p$ comme dans la définition 3. Supposons que la somme des coefficients de f n'est pas multiple de p, et notons $\mathcal{I}$ l'ensemble des valeurs non nulles des coefficients de f. Alors*

$$A_0(f,p) - A_1(f,p) = -\left(\sum_{i \in \mathcal{I}} (A_0(f \setminus < i >, p) - A_1(f \setminus < i >, p)) \right), \tag{2.23}$$

où $f \setminus < i >$ est la forme linéaire obtenue à partir de f en replaçant par zéro un coefficient égal à i.

Démonstration. On a

$$A_0(f,p) - A_1(f,p) = \frac{C_0(f,p) - C_1(f,p)}{\prod_{i\in\mathcal{I}}\ n_i(f)!}.$$

Or, d'après l'équation de Pascal pour les coefficients coloriés,

$$C_1(f,p) - C_0(f,p) = \sum_{i\in\mathcal{I}} n_i(f)(C_0(f\setminus < i >, p) - C_1(f\setminus < i >, p)) \tag{2.24}$$

$$= \sum_{i\in\mathcal{I}} n_i(f)(A_0(f\setminus < i >, p) - A_1(f\setminus < i >, p))(n_i(f)-1)! \prod_{j\in\mathcal{I}\setminus\{i\}} n_j(f)!. \tag{2.25}$$

Quand on regroupe les produits en factorielles, et on simplifie, on obtient (2.23). □

Définition 4. Une *source* est une forme linéaire dont la somme des coefficients est un multiple de p.

Remarquons que ce résultat généralise à la fois le lemme 2.2.1 et l'équation classique du triangle de Pascal. En effet, si $f(x_1,\ldots,x_n,\ldots) = x_1 + \ldots + x_n$ $(0 < n < p)$, le théorème 2.3.2 appliqué à f dit que

$$A_0(n,p) - A_1(n,p) = A_1(n-1,p) - A_0(n-1,p)$$

ce qui équivaut au Lemme 2.2.1.

2.4 La recherche des éléments des simplexes de Pascal

L'équation de Pascal (2.23) permet aussi de trouver tous les nombres $\triangle_f$. Ce chapitre est une preuve algorithmique du fait qu'étant donnés un nombre premier p et un ensemble $\mathcal{I} \subset \mathbb{F}_p^\times$, le système formé des équations de Pascal, auxquelles sont ajoutées les valeurs (déjà connues) de $\triangle_f$ pour les formes linéaires f dont l'ensemble des valeurs des coefficients est inclus strictement dans $\mathcal{I} \cup \{0\}$, avec comme inconnues les nombres $\triangle_f$, admet une solution unique. Il faut noter que, comme c'est un système d'équations linéaires avec plus d'équations que d'inconnues, chaque cas particulier peut être résolu par les moyens d'algèbre linéaire.

Considérons l'exemple générique où $p = 5$ et $\mathcal{I} = \{a, b\}, a \neq b$. Appelons les inconnues

$$x := \triangle_{ax_1+bx_2}, \tag{2.26}$$

$$y := \triangle_{ax_1+ax_2+bx_3}, \tag{2.27}$$

$$z := \triangle_{ax_1+bx_2+bx_3}; \tag{2.28}$$

alors les six équations de Pascal sont (les constantes sont les valeurs de $\triangle_f$ quand f n'a pas de coefficient égal à a, ou à b, ou à 0) :

$$\left\{\begin{array}{rll} x & = 2 & \text{(sauf si } a \equiv b) \\ y & = -1 - x & \text{(sauf si } 2a + b \equiv 0) \\ z & = -1 - x & \text{(sauf si } a + 2b \equiv 0) \\ -1 & = 1 - y & \text{(sauf si } a + 2b \equiv 0) \\ 1 & = -y - z & \text{(sauf si } a \equiv b) \\ -1 & = 1 - z & \text{(sauf si } 2a + b \equiv 0). \end{array}\right.$$

Quatre de ces équations sont conséquences du Théorème 2.3.2, et les deux autres correspondent aux sources (elles ne sont donc pas à prendre en compte), et la sélection se fait en fonction du choix de a et b (il y a 3 choix différents).

Notons que l'existence d'une solution est acquise, car les nombres $\triangle_f$ en forment une.

Maintenant, nous allons écrire notre problème formellement. Une forme linéaire f sera identifiée à la suite des nombres $(n_0(f), n_1(f), \ldots, n_{p-1}(f))$ qui vérifie $n_1 + \ldots + n_{p-1} < p$. On sait que deux formes linéaires qui correspondent au même $p-1$-uplet sont équivalentes pour notre problème. L'énoncé formulé au début de la section correspond au

Théorème 2.4.1. *Soit p un nombre premier impair, $a_1, \ldots, a_d$ des éléments différents de $\mathbb{F}_p^\times$ (on notera $\mathcal{I}$ l'ensemble $\{a_1, \ldots, a_d\}$), et $\triangle$ une fonction $\mathbb{N}^d \to \mathbb{Z}$ telle que*

$$n_1 + n_2 + \ldots + n_d \geqslant p \Rightarrow \triangle(n_1, n_2, \ldots, n_d) = 0; \tag{2.29}$$

$$\left[\begin{array}{c} \exists i, n_i = 0 \text{ ou} \\ n_1 + n_2 + \ldots + n_d = p - 1 \end{array}\right. \Rightarrow \triangle(n_1, n_2, \ldots, n_d) = \triangle_f \tag{2.30}$$

pour toute forme linéare f telle que $n_{a_1}(f) = n_1, \ldots, n_{a_d}(f) = n_d$ et $n_c(f) = 0$ si $c \notin \mathcal{I}$;

$$\text{si } \left\{\begin{array}{l} \sum_{i=1}^{d} a_i n_i \not\equiv 0 \bmod p \quad \text{et} \\ \qquad \sum_{i=1}^{d} n_i < p, \\ \text{pour tout } i, n_i > 0 \qquad \text{alors} \end{array}\right.$$

$$\triangle(n_1, n_2, \ldots, n_d) = -\sum_i \triangle(n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_d). \tag{2.31}$$

Alors $\triangle(n_1, n_2, \ldots, n_d) = \triangle_f$ pour tous $(n_1, n_2, \ldots, n_d) \in \mathbb{N}^d$ tels que $n_1 + n_2 + \ldots + n_d < p$, et pour toute application linéaire f telle que $n_{a_1}(f) = n_1, \ldots, n_{a_d}(f) = n_d$ et $n_c(f) = 0$ si $c \notin \mathcal{I}$.

Démonstration. Si $d = 1$, l'équation (2.31) s'écrit simplement $\triangle(n+1) = -\triangle(n)$ pour $n = 1, \ldots, p-2$; (2.29) et (2.30) se traduisent respectivement par $\triangle(n) = 0$ pour $n \geqslant p$ et $\triangle(0) = 1$. La seule solution de ce problème est $\triangle(n) = (-1)^n = A_0(n,p) - A_1(n,p)$ pour $0 \geqslant n \geqslant p-1$.

Si $d \geqslant 2$, on va procéder récursivement, avec comme premier critère de récurrence, $(n_1 + n_2 + \ldots + n_d)$ variera de la plus grande jusqu'à la plus petite valeur. Les points de chaque tranche qui correspond à une valeur fixe de $(n_1 + \ldots + n_d)$ (qui forment un simplexe à $d-1$ dimensions) seront divisés en segments qui correspondent aux valeurs fixes de $n_3, \ldots, n_d$, et ces segments seront traités dans l'ordre de $n_3 + \ldots + n_d$ du plus petit au plus grand.

Pour $\sum n_i = p-1$, l'énoncé vient de l'équation (2.30). Pour $h = \sum n_i < p$, considérons un segment défini par des valeurs fixes de $n_3, \ldots, n_d$ telles que $l = h - \sum_{i=3}^{d} n_i \geqslant 0$.

Alors, (2.31) définit les équations suivantes pour les variables $\triangle_i := \triangle(l-i, i, n_3, n_4, \ldots, n_d)$ $(i \in \{1, \ldots, l-1\})$:

$$\begin{cases} \triangle_0 + \triangle_1 + \displaystyle\sum_{j=2}^{d} \triangle(l, 1, n_3, \ldots, n_j - 1, \ldots, n_d) = -\triangle(l, 1, n_3, \ldots, n_d) \\ \triangle_1 + \triangle_2 + \displaystyle\sum_{j=2}^{d} \triangle(l-1, 2, n_3, \ldots, n_j - 1, \ldots, n_d) = -\triangle(l-1, 2, n_3, \ldots, n_d) \\ \qquad\qquad . \qquad . \qquad . \qquad . \qquad . \\ \triangle_{l-1} + \triangle_l + \displaystyle\sum_{j=2}^{d} \triangle(1, l, n_3, \ldots, n_j - 1, \ldots, n_d) = -\triangle(l-1, 2, n_3, \ldots, n_d) \end{cases} \tag{2.32}$$

Les valeurs de $\triangle$ autres que $\triangle_i$ sont supposées connues grâce aux hypothèses de récurrence, et les valeurs de $\triangle_0$ et $\triangle_l$ le sont grâce à (2.30). Ce système est un système de l équations de $l-1$ variables, dont au plus une équation doit être retirée, car elle correspond à une source. Indépendamment de quelle équation doit être retirée, il a au plus une solution, ce qui montre le résultat pour le segment considéré. □

La description d'un algorithme qui calcule les nombres $\triangle_f$ à partir des données d'entrée minimales (p et $\mathcal{I}$) ne sera complète que si on a une façon de calculer les valeurs de $\triangle_f$ mentionnées dans (2.30) (les valeurs aux bords). Celles-ci viennent d'une récurrence sur la dimension d. Si une forme linéaire f ne contient que $d' < d+1$ coefficients différents, on peut soustraire un coefficient des autres (ce n'est nécessaire que si f ne contient pas zéro parmi ses coefficients) et obtenir une autre forme linéaire f' telle que $\triangle_{f'} = \triangle_f$, qui n'a que $d'-1$ coefficients différents.

Les hypothèses du Théorème 2.4.1 peuvent être affaiblies, car les valeurs prescrites dans (2.30) vérifient aussi l'équation (2.31). Aux points $(n_1, n_2, \ldots, n_d)$, c'est une conséquence directe du théorème 2.3.2 si on considère que $\triangle(n_1, n_2, \ldots, -1, \ldots, n_d) = 0$, et pour les points de la facette d'équation $n_1 + n_2 + \cdots + n_d = p-1$, ce fait vient du

Théorème 2.4.2 (L'équation de Pascal impropre)**.** *Soit p un nombre premier impair, soit $f \in \mathbb{F}_p^{\times p}$ un vecteur ligne dont la somme des composantes n'est pas multiple de p, et soit $\mathcal{I}$ l'ensemble des valeurs de ses composantes. Alors*

$$0 = \sum_{i \in \mathcal{I}} (A_0(f \setminus < i >, p) - A_1(f \setminus < i >, p)) \tag{2.33}$$

où $f \setminus < i >$ désigne une (quelconque) forme linéaire qui correspond à un vecteur ligne obtenu à partir de f en retirant un coefficient égal à i.

On peut le montrer en considérant f comme une application linéaire de $\mathbb{F}_p^p$ dans $\mathbb{F}_p$ et en suivant les preuves des Théorèmes 2.3.1 et 2.3.2, ou bien en remarquant que l'équation (2.33) coïncide avec l'équation de Pascal

pour les formes $f \setminus < i > -\mathbf{i}_0$ où

$$\mathbf{i}_0(x_1, \ldots, x_{p-1}) = i_0 \cdot (x_1 + \ldots + x_{p-1}),$$

et $i_0 \in \mathcal{I}$ est fixe. Les points $(n_1, n_2, \ldots, n_d)$ tels que $n_1+n_2+\ldots+n_d = p$ et $a_1n_1+a_2n_2+\ldots+a_dn_d \equiv 0 \bmod p$, seront appelés les *sources extérieures.*

Le Théorème 2.4.1 peut donc être reformulé de façon suivante :

Théorème 2.4.3. *Soit p un nombre premier impair, $a_1, \ldots, a_d$ des éléments différents de $\mathbb{F}_p^\times$, et $\triangle$ une function $(\mathbb{N} \cup \{-1\})^d \to \mathbb{Z}$ telle que*

$$n_1 + n_2 + \ldots + n_d \geqslant p \Rightarrow \triangle(n_1, n_2, \ldots, n_d) = 0; \tag{2.34}$$

$$\exists i, n_i < 0 \Rightarrow \triangle(n_1, n_2, \ldots, n_d) = 0; \tag{2.35}$$

$$\triangle(0, 0, \ldots, 0) = 1; \tag{2.36}$$

si $(n_1, \ldots, n_d) \in \mathbb{N}^d$ et $\sum_{i=1}^{d} a_i n_i \not\equiv 0 \bmod p$ alors

$$\triangle(n_1, n_2, \ldots, n_d) = -\sum_i \triangle(n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_d). \tag{2.37}$$

Alors $\triangle(n_1, n_2, \ldots, n_d) = \triangle_f$ pour tous $(n_1, n_2, \ldots, n_d) \in \mathbb{N}^d$ tels que $n_1 + n_2 + \ldots + n_d < p$, et pour toute forme linéaire f telle que $n_{a_1}(f) = n_1, \ldots, n_{a_d}(f) = n_d$ et $n_c(f) = 0$ si $c \notin \mathcal{I}$.

Le pseudo-code ci-dessous correspond à l'algorithme "d'attaque par le fond" décrit dans la preuve du Théorème 2.4.1 pour la dimension $d = 2$. Les données d'entrée de l'algorithme sont des entiers p, a, b tels que p est premier et $0 < a < b < p$.

Ce pseudo-code utilise la notation du type data$[x][y]$ = ... pour désigner l'écriture dans un tableau mais la notation du type $y \leftarrow n - x$ pour désigner l'écriture dans une des variables de comptage x, y, n. Le but est de souligner le fait que chaque case des tableaux fait l'objet d'une seule écriture (et de trois lectures au maximum). Remarquons que ce pseudo-code simpliste utilise deux fois plus de mémoire que nécessaire, car les seules données intéressantes qu'il calcule sont data$[x][y]$ pour $x + y \leqslant p - 1$.

À titre d'exemple, pour $p = 11, a = 1, b = 3$, cet algorithme produit le triangle de la page 58.

Algorithme 1 Calculer un triangle de Pascal fini. Arguments $p, a, b : p$ premier, $0 < a < b < p$

création des tableaux,
data *contiendra les nombres du triangle de Pascal,*
reg *vaudra* true *ssi le point n'est pas une source,*
aucune donnée de ces tableaux ne sera réécrite deux fois.
Créer le tableau data$[0..p-1][0..p-1]$
Créer le tableau reg$[0..p-1][0..p-1]$
for $x = 0, .., p-1, y = 0, .., p-1$ **do**
    reg$[x][y] = (a \cdot x + b \cdot y \not\equiv 0 \bmod p)$
end for
résolution des sommets
data$[0][0]$ =data$[p-1][0]$ =data$[0][p-1] = 1$
résolution des côtés
for $x = 1, .., p-2$ **do**
    data$[x][p-1-x] = -$data$[x-1][p-x]$
end for
for $x = 1, .., p-2$ **do**
    data$[x][0] = -$data$[x-1][0]$
end for
for $y = 1, .., p-2$ **do**
    data$[0][y] = -$data$[0][y-1]$
end for
résolution à l'intérieur
for $n = p-2, .., 1$ **do**
    for $x = 1, .., n-1$ **do**
        $y \leftarrow n - x$
        if reg$[x][y+1]$ **then**
            data$[x][y] = -$data$[x-1][y+1] -$ data$[x][y+1]$
        else
            Arrêter la boucle
        end if
    end for
    for $y = 1, .., n-1$ **do**
        $x \leftarrow n - y$
        if reg$[x+1][y]$ **then**
            data$[x][y] = -$data$[x+1][y-1] -$ data$[x+1][y]$
        else
            Arrêter la boucle
        end if
    end for
end for
impression du résultat
for $n = 0, .., p-1$ **do**
    for $y = 0, .., n$ **do**
        Imprimer data$[n-y][y]$, reg$[n-y][y]$
    end for
    Passage à la ligne
end for

2.5 Applications et prolongements

Dans ce chapitre, on verra l'utilisation de la théorie précédente dans l'étude des exposants de raréfaction, dont la formule a été trouvée dans le chapitre 1.1 ; on traitera aussi le cas particulier formulé dans le chapitre 1.2.

Remarquons d'abord que l'équation (2.37) peut être remplacée dans le Théorème 2.4.3 par n'importe quelle équation de type

$$-\triangle(n_1, n_2, \ldots, n_d) = \sum_i c_i \triangle(n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_d),$$

et la solution correspondante sera

$$\triangle(n_1, n_2, \ldots, n_d) = \prod_i c_i^{n_i} \triangle_f$$

où f désigne n'importe quelle forme linéaire qui correspond à $(n_1, \ldots, n_d)$.

Soient $P(x) = 1 + c_1 x + c_2 x^2 + \ldots + c_d x^d$ un polynôme tel que $P(0) = 1$ et $p > d$ un nombre premier. On va exprimer les valeurs des polynômes symétriques élémentaires en nombres $P(\zeta)$ (où ζ parcourt les racines primitives p-ièmes de l'unité) en termes des structures étudiées ci-dessus. Si le polynôme symétrique étudié est le produit de $p-1$ nombres, en développant ce produit, on obtient l'identité suivante dans $\mathbb{Z}[X]/(X^p - 1)$

$$\prod_{j \in \mathbb{F}_p^\times} (P(X^j)) = S_0 + S_1 X + S_2 X^2 + \ldots + S_{p-1} X^{p-1},$$

où

$$S_i = \sum_{n_1, n_2, \ldots, n_d} \prod_{j=1}^{d} c_j^{n_j} A_i(f_{n_1, \ldots, n_d}, p); \tag{2.38}$$

la dernière somme parcourt tous les $(n_1, \ldots, n_d) \in \mathbb{N}^d$ tels que $n_1 + \ldots + n_d < p$, et $f_{n_1, \ldots, n_d}$ est une forme linéaire de $\mathbb{F}_p^{p-1}$ à valeurs dans $\mathbb{F}_p$ telle que $n_j(f) = n_j$. On a ensuite :

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(P(\zeta)) = S_0 - S_1 = \sum_f \prod_{j=1}^{d} c_j^{n_j(f)} \triangle_f. \tag{2.39}$$

Par conséquent, il suffit de construire le simplexe de Pascal de dimension d et de taille p qui correspond à $\mathcal{I} = \{1, \ldots, d\}$, puis ajouter ses éléments multipliés par les coefficients $\prod c_j^{n_j}$ pour calculer la norme de $P(\zeta)$.

Le développement du polynôme symétrique $\sigma_{p-1-\delta}$ (avec $\delta \in \{0, \ldots, p-2\}$) peut être écrit

$$\sigma_{p-1-\delta}(P(X), P(X^2), \ldots, P(X^{p-1})) = S_0 + S_1 X + S_2 X^2 + \ldots + S_{p-1} X^{p-1},$$

où

$$S_i = \sum_{\substack{X^* \subset \mathbb{F}_p^\times, \\ |X^*| = \delta}} \sum_{n_1, n_2, \ldots, n_d} \prod_{j=1}^{d} c_j^{n_j} A_i^{\mathbb{F}_p^\times \setminus X^*}(f_{n_1, \ldots, n_d}, p); \tag{2.40}$$

ici, $A_i^{\mathbb{F}_p^\times \setminus X^*}(f_{n_1, \ldots, n_d}, p)$ est le nombre de solutions de la congruence $f_{n_1, \ldots, n_d} \equiv i \bmod p$ avec $x_i \in \mathbb{F}_p^\times \subset X^*$ deux à deux différents. Remarquons que $S_1 = S_2 = \ldots = S_{p-1}$, mais les nombres $A_i^{\mathbb{F}_p^\times \setminus X^*}(f_{n_1, \ldots, n_d}, p)$ sont à priori différents pour tous les i. La somme (2.40) se regroupe dans

$$S_i = \sum_{n_1, n_2, \ldots, n_d} \prod_{j=1}^{d} c_j^{n_j} \sum_{\substack{X^* \subset \mathbb{F}_p^\times, \\ |X^*| = \delta}} A_i^{\mathbb{F}_p^\times \setminus X^*}(f_{n_1, \ldots, n_d}, p) = \sum_{n_1, n_2, \ldots, n_d} \prod_{j=1}^{d} c_j^{n_j} \binom{n_0}{\delta} A_i(f_{n_1, \ldots, n_d}, p),$$

où $n_0 = p-1-n_1-n_1-\ldots-n_d$, car chaque solution de la congruence modulo p apparaît $\binom{n_0}{\delta}$ fois. On en déduit la formule

$$\sigma_{p-1-\delta}(P(\zeta)) = \sum_f \prod_{j=1}^{d} c_j^{n_j(f)} \binom{n_0(f)}{\delta} \triangle_f. \tag{2.41}$$

Si certains des c_j sont nuls, on peut enlever les indices correspondants de $\mathcal{I}$, et travailler en dimension plus petite.

2.5.1 La norme de $(1-\zeta)$

Cette conséquence du Lemme 2.2.1 possède une preuve beaucoup plus simple.

Corollaire 2.5.1. *Soit p un nombre premier et ζ une racine primitive p-ième de l'unité. Alors,*

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = p.$$

Démonstration. La formule (2.39) prend la forme

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = \sum_{n=0}^{p-1} (-1)^n (A_0(n,p) - A_1(n,p)).$$

D'après le Lemme 2.2.1, cette somme est égale à p. □

2.5.2 La norme de $(1+\zeta-\zeta^2)$

Nous allons montrer le résultat suivant :

Théorème 2.5.2. *Soit p un nombre premier et ζ une racine primitive p-ième de l'unité. Alors,*

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1+\zeta-\zeta^2) = L_p, \tag{2.42}$$

où L_n sont les nombres de Lucas définis par

$$L_0 = 2,$$
$$L_1 = 1,$$

et pour tout $n \in \mathbb{N}$

$$L_{n+2} = L_n + L_{n+1}. \tag{2.43}$$

C'est la suite A000032 d'OEIS. D'après le livre [3], L_p est le nombre de façons de placer des "dominos" (c'est à dire des sous-ensembles de la forme $\{k, k+1\}$) disjoints sur le cercle $\mathbb{Z}/p\mathbb{Z}$.

Démonstration. Calculons d'abord les nombres $\triangle_f$ quand $\mathcal{I} = \{1,2\}$. Dans le triangle correspondant (le triangle marqué par "$n_0 = 0$" dans l'Annexe 4 en est le cas particulier où $p = 11$; les sources du triangle sont marquées par des losanges), toutes les $\frac{p-1}{2}$ sources sont alignées, ce qui permet d'utiliser un algorithme plus simple que celui décrit dans le chapitre 2.4.

Pour calculer les nombres $\triangle_f$ au-dessus de la droite des sources, appliquons successivement l'équation de Pascal (2.23) en partant du sommet de haut, et sous la ligne des sources, mettons-la sous la forme

$$\triangle_{f\backslash<1>} = \triangle_f - \triangle_{f\backslash<2>}, \tag{2.44}$$

et appliquons-la successivement à partir du sommet inférieur-droit. Remarquons que l'équation (2.44) est aussi valable si $f\backslash<1>$ est une source.

La réunion de ces deux méthodes montre le résultat suivant : si $n_1(f) + 2n_2(f) < p$ (c'est à dire, f est au-dessus de la droite des sources),

$$\triangle_f = (-1)^{n_0(f)} \binom{n_1(f) + n_2(f)}{n_1(f)} \tag{2.45}$$

(ce qui est un cas particuler de (2.14)), et si $n_1(f) + 2n_2(f) \geqslant p$ (f est une source ou sous cette droite),

$$\triangle_f = (-1)^{n_2(f)} \binom{n_0(f) + n_1(f)}{n_0(f)}. \tag{2.46}$$

Par conséquent,

$$N(1+\zeta-\zeta^2) = \sum_{n_0=0}^{p-1} \left(\sum_{n_2=0}^{\min(p-1-n_0,n_0)} (-1)^{p-1-n_0-n_2} \binom{p-1-n_0}{n_2} + \sum_{n_2=n_0+1}^{p-1-n_0} \binom{p-1-n_2}{n_0} \right). \tag{2.47}$$

Pour montrer que l'expression (2.47) vaut L_p, nous allons identifier les termes de cette somme à des nombres de façons de placer des dominos sur $\mathbb{F}_p$ avec des restrictions. Les termes de la première somme, qui correspondent à $n_0 = \frac{p-1}{2}, \ldots, p-2$ sont nuls, et le terme correspondant à $n_0 = p-1$ vaut un. De plus, chaque terme correspondant à $n_0 = 0, \ldots, \frac{p-3}{2}$ vaut le nombre de façons de placer n_0+1 dominos sur le cercle $\mathbb{Z}/p\mathbb{Z}$.

Pour montrer cela, considérons que le premier domino est le premier domino qu'on rencontre en parcourant la suite $0, 1, 2, \ldots$ des points du cercle. Si aucun domino n'est situé à la position $'(p-1)$—$0'$, supposons que le premier domino se trouve en $'(n_2 - n_0 - 1)$—$(n_2 - n_0)'$, ce qui laisse $(p - 1 - n_2 + n_0)$ cases après lui pour les n_0 dominos restants. Le nombre de façons de placer n_0 dominos sur un "segment de droite" de longueur $p - 1 - n_2 + n_0$ est égal exactement à $\binom{p-1-n_2+n_0-n_0}{n_0}$ c'est à dire à un terme de la dernière somme de (2.47).

La deuxième somme de (2.47) peut être rendue plus compacte par la formule

$$\sum_{k=0}^{m} (-1)^{k+n} \binom{n}{k} = (-1)^{m+n} \binom{n-1}{m}.$$

Donc, si $n_0 < \frac{p-1}{2}$, la deuxième somme de (2.47) est égale à

$$\sum_{n_2=0}^{\min(p-1-n_0,n_0)} (-1)^{n_0+n_2} \binom{p-1-n_0}{n_2} = \binom{p-2-n_0}{n_0},$$

c'est à dire au premier terme de la troisième somme, qui lui-même vaut le nombre de placements de $n_0 + 1$ dominos avec un domino en position $'0$—$1'$. On peut identifier ce terme avec le nombre de placements de $n_0 + 1$ dominos avec un domino en position $'(p-1)$—$0'$, ce qui termine le dénombrement des placements possibles de dominos sur le cercle $\mathbb{Z}/p\mathbb{Z}$.

□

D'après ce résultat, si $p > 3$ est tel que 3 est un générateur de $\mathbb{F}_p^\times$, l'exposant de croissance des sommes p-raréfiées de la suite "++-" est

$$\frac{\log L_p}{(p-1)\log 3}. \tag{2.48}$$

2.5.3 Norme de $(1-\zeta+\zeta^2)$

Dans cette partie, nous allons calculer la norme de $P(\zeta) = 1-\zeta+\zeta^2$ directement, puis faire le lien avec la preuve précédente.

Théorème 2.5.3. *Soit n un entier supérieur à 4 qui n'est multiple ni de 2 ni de 3, et soit $\zeta = e^{\frac{2i\pi}{n}}$. Alors,*

$$\prod_{k=1}^{n-1}(1-\zeta^k+\zeta^{2k}) = 1.$$

Par conséquent, $1-\zeta+\zeta^2$ est une unité de l'anneau des entiers de $\mathbb{Q}(\zeta)$.

Démonstration. Pour chaque $k \in [1, n-1]$, on a

$$1-\zeta^k+\zeta^{2k} = \zeta^k\left(\zeta^k+\zeta^{-k}-1\right) = \zeta^k(2\cos\frac{2\pi k}{n}-1) = \zeta^k\frac{\cos\frac{3\pi k}{n}}{\cos\frac{\pi k}{n}}.$$

Le produit des termes ζ^k vaut un, et on peut vérifier que les produits $\prod_{k=1}^{n-1}\cos\frac{3\pi k}{n}$ et $\prod_{k=1}^{n-1}\cos\frac{3\pi k}{n}$ sont les mêmes à une permutation des facteurs près. □

Ce résultat admet le corollaire combinatoire suivant :

Corollaire 2.5.4. *Soit p un nombre premier, $p \geqslant 5$. Alors, le nombre de façons de placer un nombre pair et non nul de dominos sur le cercle de longueur p est égal au nombre de façons de placer un nombre de dominos impair sur ce cercle.*

Démonstration. Les formules (2.45), (2.46) et

$$(-1)^{n_1(f)}\triangle_f = (-1)^{n_0(f)}\cdot(-1)^{n_2(f)}\triangle_f$$

impliquent :

$$N(1-\zeta+\zeta^2) = \sum_{n_0=0}^{p-1}(-1)_0^n\left(\sum_{n_2=0}^{\min(p-1-n_0,n_0)}(-1)^{p-1-n_0-n_2}\binom{p-1-n_0}{n_2}+\sum_{n_2=n_0+1}^{p-1-n_0}\binom{p-1-n_2}{n_0}\right), \tag{2.49}$$

c'est à dire

$$0 = \sum_{n_0=1}^{\frac{p-3}{2}}(-1)_0^n\left(\binom{p-2-n_0}{n_0}+\sum_{n_2=n_0+1}^{p-1-n_0}\binom{p-1-n_2}{n_0}\right).$$

Le résultat vient du fait que chaque terme entre parenthèses est égal au nombre de façons de placer n_0 dominos sur le cercle de longueur p.

□

Par exemple, pour $p = 11$, il y a :
1 façon de placer 0 dominos sur un cercle de longueur 11 ;
11 façons de placer 1 domino ;
44 façons de placer 2 dominos ;
77 façons de placer 3 dominos ;
55 façons de placer 4 dominos ;
11 façons de placer 5 dominos.

Pour $p = 17$, il y a :
1 façon de placer 0 dominos sur un cercle de longueur 17 ;
17 façons de placer 1 domino ;
119 façons de placer 2 dominos ;
442 façons de placer 3 dominos ;
935 façons de placer 4 dominos ;
1122 façons de placer 5 dominos ;
714 façons de placer 6 dominos ;
204 façons de placer 7 dominos ;
17 façons de placer 8 dominos.

2.5.4 Les avant-derniers coefficients des polynômes annulateurs de $(1 + \zeta - \zeta^2)$ et de $(1 + \zeta - \zeta^2)(1 + \zeta^{b'} - \zeta^{2b'})$

Retournons à l'étude du phénomène de Newman pour la suite "++−", commencée dans la partie 1.4. Nous pouvons maintenant montrer facilement le résultat suivant :

Corollaire 2.5.5. *Soient un nombre premier $p > 5$ et un entier $\delta \in \{0, \dots, p-2\}$. Alors $\sigma_{p-1-\delta}(1+\zeta-\zeta^2)$ (la valeur du polynôme symétrique élémentaire de degré $(p-1-\delta)$ des nombres $(1+\zeta-\zeta^2)$ où ζ parcourt les racines primitives p-ièmes de l'unité) vaut $\binom{p-1}{\delta}$ plus la somme des "poids" des façons de placer un nombre $n > 0$ dominos sur un cercle de longueur p, les poids étant $\binom{n-1}{\delta}$.*

En particulier,

$$\sigma_{p-1-\delta}(1 + \zeta - \zeta^2) > 0.$$

Démonstration. D'après (2.41),

$$\sigma_{p-1-\delta}(1 + \zeta - \zeta^2) = \sum_{n_0=0}^{p-1} \binom{n_0}{\delta} \sum_{n_2=0}^{p-1-n_0} (-1)^{n_2} \triangle_f$$

où f est une forme linéaire sur ${\mathbb{F}_p}^{p-1}$ telle que $n_0(f) = n_0, n_1(f) = p - 1 - n_0 - n_2, n_2(f) = n_2$. Ensuite, d'après la preuve du Théorème 2.5.2, si $n_0 < p - 1$, la deuxième somme vaut le nombre de façons de placer $n_0 + 1$ dominos sur un cercle de longueur p. □

L'étude de la valeur du polynôme symétrique $\sigma_{p-2}\big((1 + \zeta - \zeta^2)(1 + \zeta^{b'} - \zeta^{2b'})\big)$ à l'aide de la formule (2.41) demande de traiter un tableau 8-dimensionnel d'entiers. Une autre approche consiste à exploiter la structure du polynôme pour se ramener à un problème qui ressemble au Problème 1 avec deux valeurs de coefficients possibles. Explicitons cette approche.

Le développement de $\sigma_{p-2}\big((1+\zeta-\zeta^2)(1+\zeta^{b'}-\zeta^{2b'})\big)$ s'écrit

$$\sum_{x^*=1}^{p-1}\frac{1}{((1+\zeta^{x^*}-\zeta^{2x^*})(1+\zeta^{b'x^*}-\zeta^{2b'x^*}))}\prod_{j=1}^{p-1}\big((1+\zeta^j-\zeta^{2j})^2(1+\zeta^{b'j}-\zeta^{2b'j})^2\big)=$$
$$L_p\sum_{x^*=1}^{p-1}\frac{1}{((1+\zeta^{x^*}-\zeta^{2x^*})(1+\zeta^{b'x^*}-\zeta^{2b'x^*}))}\prod_{j=1}^{p-1}\big((1+\zeta^j-\zeta^{2j})(1+\zeta^{b'j}-\zeta^{2b'j})\big), \tag{2.50}$$

et, comme $b'\not\equiv 1$, aucune fraction rationnelle n'apparaît dans la partie de droite. Cela constitue une preuve directe du fait que $\sigma_{p-2}\big((1+\zeta-\zeta^2)(1+\zeta^{b'}-\zeta^{2b'})\big)$ est multiple de L_p, et aussi une description combinatoire de la valeur de leur quotient. Elle motive, en fait, le problème suivant :

Problème 3. *Calculer le nombre de solutions d'un système de congruences linéaires*

$$\begin{cases} f_1x_1+f_2x_2+\ldots+f_nx_n & =i\\ b'x_{p-2}-x_{p-1} & =0\end{cases} \tag{2.51}$$

dans $\mathbb{F}_p^{n+2}$ (où $n\leqslant p-3$, b' est un générateur du groupe multiplicatif $\mathbb{F}_p^\times$, et i est un élément fixe de $\mathbb{F}_p$) qui n'utilisent ni zéro ni deux fois un même élément de $\mathbb{F}_p^\times$.

Notons qu'on peut, comme au début de la partie 3.3, écrire la première équation du système (2.51) comme $f(x_1,x_2,\ldots,x_{p-3})=i$, où f est une forme linéaire de $\mathbb{F}_p^{p-3}$, identifiée de façon unique par la donnée des sous-ensembles $N_j=N_j(f)=\big\{k\in\{1,\ldots,p-3\}\big|f_k=j\big\}$ de $\{1,\ldots,p-3\}$ puis définir les grandeurs

$$B_i^{(b')}(f,p):=\#\left\{\sigma\in\mathcal{S}_{p-1}\;\middle|\;\begin{cases} f(x_{\sigma(1)},\ldots,x_{\sigma(p-3)})=i\\ b'x_{p-2}-x_{p-1}=0\end{cases}\right\}, \tag{2.52}$$

$$C_i^{(b')}(f,p):=\#\left\{\sigma\in\mathcal{S}_{p-1}/\mathcal{S}(N_0)\;\middle|\;\begin{cases} f(x_{\sigma(1)},\ldots,x_{\sigma(p-3)})=i\\ b'x_{p-2}-x_{p-1}=0\end{cases}\right\}\text{ et} \tag{2.53}$$

$$A_i^{(b')}(f,p):=\#\left\{\sigma\in\mathcal{S}_{p-1}/\mathcal{S}(N_0)\mathcal{S}(N_1)\ldots\mathcal{S}(N_{p-1})\;\middle|\;\begin{cases} f(x_{\sigma(1)},\ldots,x_{\sigma(p-3)})=i\\ b'x_{p-2}-x_{p-1}=0\end{cases}\right\}. \tag{2.54}$$

Les nombres $B_i^{(b')}(f,p)$ sont égaux entre eux pour tout $i\in\mathbb{F}_p^\times$, de même pour $C_i^{(b')}(f,p)$ et $A_i^{(b')}(f,p)$. Ils vérifient aussi la formule (2.13). Notons $\triangle_f^{(b')}:=A_0^{(b')}(f,p)-A_1^{(b')}(f,p)$.

Par un calcul similaire à celui mené au début de la partie 3.5, on peut déduire de la formule (2.50) que

$$\frac{1}{L_p}\sigma_{p-2}\big((1+\zeta-\zeta^2)(1+\zeta^{b'}-\zeta^{2b'})\big)=\sum_f(-1)^{|N_2(f)|}\triangle_f^{(b')},$$

où la somme est prise sur toutes les formes linéaires de $\mathbb{F}_p^{p-3}$ à coefficients $0,1$ ou 2.

Autant l'équation de Pascal (Théorème 2.3.2) répond de façon satisfaisante au Problème 1, autant le Problème 3 est largement ouvert, même pour une forme linéaire à coefficients 0 ou 1. Par des techniques analogues à celles de la partie 3.2, on peut montrer le résultat suivant :

Théorème 2.5.6. *Soit f une forme linéaire de $\mathbb{F}_p^{p-3}$ de la forme*

$$f(x_1,x_2,\ldots,x_{p-3})=x_1+x_2+\ldots+x_n.$$

et soit un entier $b'\geqslant 3$. Alors

$$A_0^{(b')}(f,p)-A_1^{(b')}(f,p)=(-1)^np+F(n) \tag{2.55}$$

pour tout premier p assez grand (indépendamment de si b' est un générateur du groupe multiplicatif $\mathbb{F}_p^\times$). On notera, par analogie avec la partie 3.2, $A_i^{(b')}(f,p)=A_i^{(b')}(n,p)$.

Démonstration. Nous allons appliquer la formule d'inversion de Möbius à un ensemble partiellement ordonné plus grand que dans la preuve du Lemme 2.2.1, qui garde l'information sur toutes les relations de type $x_i = x_j$ ou $x_i = b'x_j$ dans une suite de classes résiduelles non nulles modulo p. Soit Γ_n le sous-ensemble de $(B^{\mathbb{N}}X_1 \cup B^{\mathbb{N}}X_2 \cup \ldots \cup B^{\mathbb{N}}X_n)^n/\mathcal{S}(X_1, \ldots, X_n)$ (où $B, X_1, \ldots, X_n$ sont des variables formelles) formé des classes d'équivalence de telles suites que les exposants de B devant chaque variable X_k forment un ensemble de type $\{0, 1, \ldots, l\}$; un élément de Γ_n sera appelé un système de relations d'égalité ou de proportionnalité (par le rapport b'). L'ordre sur l'ensemble Γ_n sera défini de façon suivante : si $\bar{\sigma}, \bar{\pi} \in \Gamma_n$, on dira que $\bar{\sigma} \geqslant \bar{\pi}$ si (après un choix adapté de représentants σ et π) on peut remplacer certaines variables $X_{j_1}, X_{j_2}, \ldots, X_{j_k}$ (et toutes leurs occurrences) dans π par des monômes de type $B^{n_1}X_{i_1}, B^{n_2}X_{i_2}, \ldots, B^{n_k}X_{i_k}$ respectivement, où X_{i_l} sont des variables, présentes dans π, différentes des $X_{j_{l'}}$, et obtenir σ.

Définissons la notion qui correspond à la préimage d'une suite $(x_1, \ldots, x_n)$ d'élements de $\mathbb{F}_p^\times$ par l'algorithme suivant : soit $u(1) = (X_1, \ldots, X_n)$. Pour i qui va de 2 jusqu'à n exécuter les instructions suivantes qui définissent des suites $u(2), u(3), \ldots, u(n) \in (B^{\mathbb{N}}X_1 \cup B^{\mathbb{N}}X_2 \cup \ldots \cup B^{\mathbb{N}}X_n)^n$:
I1 : pour tout j, $u(i)_j \leftarrow u(i-1)_j$;
I2 : s'il existe $j < i$ tel que $x_i = x_j$, poser $u(i)_i \leftarrow u(i-1)_j$ et passer à l'itération suivante de la boucle ;
I3 : s'il existe $j < i$ tel que $x_i = b'x_j$, poser $u(i)_i \leftarrow Bu(i-1)_j$;
I4 : s'il existe $j < i$ tel que $b'x_i = x_j$, remplacer dans $u(i)$ toutes les occurences de $u(i-1)_j$ par $Bu(i)_i$.

Si l'ordre de b' dans le groupe multiplicatif $\mathbb{F}_p^\times$ est supérieur à n (ce qui sera une hypothèse dans la suite et ce qui est vrai pour $p > b'^n$), cet algorithme vérifie la propriété de complétude suivante : pour tout couple d'entiers $i, j \in \{1, \ldots, k\}$,

$$x_i = x_j \text{ si et seulement si } u(k)_i = u(k)_j, \text{ et}$$
$$x_i = b'x_j \text{ si et seulement si } u(k)_i = Bu(k)_j.$$

On va appeler *préimage* de la suite $(x_1, \ldots, x_n)$ la classe d'équivalence dans Γ_n de $u(n)$ et on va la noter $u(x_1, \ldots, x_n)$.

Remarquons que la structure de Γ_n est très différente de la structure de Π_n. Γ_n possède le plus petit élément $(X_1, X_2, \ldots, X_n)$ mais ne possède pas le plus grand élément, par exemple, pour $n = 2$, les classes d'équivalence de (X, X), de (X, BX) et de (BX, X) sont toutes maximales. Γ_n est, en fait, un semi-treillis inférieur : toute paire d'éléments distincts possède une unique borne inférieure maximale.

Chaque $\bar{\sigma} \in \Gamma_n$ définit une partition de $\{1, 2, \ldots, n\}$ qui est la préimage (au sens des partitions) de la fonction qui associe à k le nom de la variable parmi $X_1, \ldots, X_n$ qui apparaît dans σ_k (où σ est un représentant de $\bar{\sigma}$). Cette partition ne dépend pas du représentant, et on va appeler $c(\bar{\sigma})$ son nombre de blocs. Comme le nombre de blocs est invariant par permutation de la suite σ, on peut définir non seulement le nombre de blocs d'un élément de Γ_n ou d'une suite de résidus non nuls modulo p, mais aussi celui d'un sous-ensemble X de $\mathbb{F}_p^\times$. Dans ce cas, les blocs sont les classes associées à la relation d'équivalence induite sur X par les relations $x_i \sim x_j$ si $x_i = b'x_j$.

On aura aussi besoin de définir un sous-ensemble spécial $\mathcal{P}_n$ de Γ_n constitué de systèmes *injectifs :* on dira que $\bar{\sigma} \in \Gamma_n$ est un élément de $\mathcal{P}_n$ si pour tous $i \neq j$ dans $\{1, \ldots, n\}$ et tout représentant σ de la classe d'équivalence $\bar{\sigma}$ on a $\sigma_i \neq \sigma_j$. On peut vérifier que $\mathcal{P}_n$ est un idéal de l'ensemble partiellement ordonné Γ_n. De plus, si Σ est un élément maximal de $\mathcal{P}_n$ (ce qui équivaut à dire que que $\Sigma \in \mathcal{P}_n$ et Σ est un élément maximal de Γ_n, ou que Σ est un élément de $\mathcal{P}_n$ avec un seul bloc), alors l'idéal engendré par $\{\Sigma\}$ est isomorphe à l'ensemble partiellement ordonné des sous-ensembles d'un ensemble de $n-1$ éléments.

Donnons maintenant une autre définition des nombres $A_i^{(b')}(n, p)$. Ils comptent les sous-ensembles de $\mathbb{F}_p^\times$ de

taille n et de somme i, en comptant chaque sous-ensemble X autant de fois qu'il y a de couples $(x^*, b'x^*)$ dans $\mathbb{F}_p^\times \setminus X$. On peut compter les couples interdits bloc par bloc de X : chaque $x \in X$ interdit le couple $(x, b'x)$, de plus, chaque bloc B possède exactement un élément x tel que $\frac{x}{b'} \notin X$ (car l'ordre de b' est supérieur à n), donc le bloc B interdit $|B|+1$ couples de cette façon, et ceux-ci ne sont pas interdits par un autre bloc. En tout, le nombre de couples $(x^*, b'x^*)$ interdits par une partie X vaut $|X| + c(X)$, et X compte avec poids $(p-1-n-c(X))$ dans un des nombres $A_i^{(b')}(n,p)$.

En passant des sous-ensembles aux suites d'éléments de $\mathbb{F}_p^\times$ on obtient :

$$n!(A_0^{(b')}(n,p) - A_1^{(b')}(n,p)) = \sum_{\sigma \in \mathcal{P}_n} \big(p-1-n-c(\sigma)\big) \Big(r_0^{(b')}(\sigma,p) - r_1^{(b')}(\sigma,p)\Big) \tag{2.56}$$

où

$$r_i^{(b')}(\sigma,p) = \#\left\{(x_1,\dots,x_n) \in \mathbb{F}_p^{\times n} \Big| \sum_k x_k = i \text{ et } u(x_1,\dots,x_n) = \sigma\right\}$$

pour chaque $i \in \mathbb{F}_p$. Notons aussi $r^{(b')}(\sigma,p) := r_0^{(b')}(\sigma,p) - r_1^{(b')}(\sigma,p)$.

À présent, nous allons faire une manœvre analogue à la Proposition 2.2.3. Appelons, pour chaque $\pi \in \Gamma_n$,

$$s^{(b')}(\pi,p) = \sum_{\sigma \geqslant \pi} r^{(b')}(\sigma,p).$$

D'après la Proposition 2.2.2, si la somme des coefficients devant chaque variable X_j présente dans π, évaluée (en tant que polynôme d'une variable) en $B = b'$ n'est pas multiple de p, on a

$$s^{(b')}(\pi,p) = (-1)^{c(\pi)}.$$

L'hypothèse précédente est vérifiée, par exemple, si $p > 1 + b' + \ldots + b'^{n-1}$.

Sous les hypothèses formulées plus haut, on a pour tout $\sigma \in \Gamma_n$:

$$r^{(b')}(\sigma,p) = \sum_{\pi \geqslant \sigma} \mu(\sigma,\pi) s(y,p) = \sum_{\pi \geqslant \sigma} (-1)^{c(\pi)} \mu(\sigma,\pi) =: G(n,\sigma) \tag{2.57}$$

où μ est la fonction de de Möbius associée à l'ensemble Γ_n. Ce nombre ne dépend ni de p ni de b'.

En injectant (2.57) dans (2.56) on obtient :

$$A_0^{(b')}(n,p) - A_1^{(b')}(n,p) = \frac{1}{n!} \sum_{\sigma \in \mathcal{P}_n} \big(p-1-n-c(\sigma)\big) G(n,\sigma) \tag{2.58}$$

$$= \sum_{\sigma \in \mathcal{P}_n} \frac{G(n,\sigma)}{n!} p - \sum_{\sigma \in \mathcal{P}_n} \big(n+1+c(\sigma)\big) \frac{G(n,\sigma)}{n!}. \tag{2.59}$$

D'après le lemme 2.2.1, on a $\sum_{\sigma \in \mathcal{P}_n} \frac{G(n,\sigma)}{n!} = (-1)^n$, d'où le résultat si on pose $F(n) = -\sum_{\sigma \in \mathcal{P}_n} \big(n+1+c(\sigma)\big) \frac{G(n,\sigma)}{n!}$.

□

La partie de cette preuve qui justifie le coefficient $(p-1-n-c(X))$ admet une rédaction en termes de théorie des graphes, mais il n'est pas clair si cela simplifie la présentation. Cette preuve donne aussi un algorithme pour calculer $F(n)$. Les premières valeurs permettent de conjecturer que $F(n) = (-1)^{n+1}\binom{n+2}{2}$.

2.6 Le problème inverse

Le Théorème 2.4.3 présente les nombres $\triangle_f$ comme la solution d'une équation en différences finies dans un domaine en forme de simplexe privé de quelques points-sources, et le nombre d'équations dans le système obtenu est supérieur au nombre d'inconnues. Remarquons que le nombre de sources est une fonction uniquement de p et de d, et les résidus $a_1, a_2, \ldots, a_d$ n'influencent que leur position. C'est une conséquence de la proposition suivante analogue à la proposition 2.2.2.

Proposition 2.6.1. *Soient p un nombre premier et d un entier tels que $p > d \geqslant 0$. Soient $a_1, \ldots, a_d$ des éléments distincts de $\mathbb{F}_p^\times$. Pour chaque $i \in \mathbb{F}_p$, notons $F_i\Big((a_1, \ldots, a_d), p\Big) = F_i(\mathbf{a}, p)$ le nombre de solutions du système*

$$\left\{ \begin{array}{l} 0 \leqslant n_1, n_2, \ldots, n_d \leqslant p \\ n_1 + n_2 + \ldots + n_d \leqslant p \\ a_1 n_1 + a_2 n_2 + \ldots + a_d n_d \equiv i \bmod p. \end{array} \right.$$

Alors,

$$F_0(\mathbf{a}, p) - F_i(\mathbf{a}, p) = 1 \tag{2.60}$$

pour tout $i \in \mathbb{F}_p^\times$.

Démonstration. Par récurrence sur d. Les cas $d = 0$ et $d = 1$ peuvent être traités directement, supposons donc que $d > 1$ et la Proposition 2.6.1 a été démontrée en dimension $d-1$. Nous allons comparer les nombres $F_i(\mathbf{a}, p)$ avec des nombres définis de la même façon dans un simplexe translaté.

Supposons sans perte de généralité que $a_1 = 1$. Alors, pour tout $i \in \mathbb{F}_p$, $F_i(\mathbf{a}, p)$ est le nombre de solutions du système

$$\left\{ \begin{array}{l} 1 \leqslant n_1 \leqslant p + 1 \\ 0 \leqslant n_2, \ldots, n_d \leqslant p \\ n_1 + n_2 + \ldots + n_d \leqslant p + 1 \\ n_1 + a_2 n_2 + \ldots + a_d n_d \equiv i + 1 \bmod p, \end{array} \right.$$

donc

$$F_{i-1}(\mathbf{a}, p) - F_i(\mathbf{a}, p) = \# \left\{ \begin{array}{l} 1 \leqslant n_1 \leqslant p + 1 \\ 0 \leqslant n_2, \ldots, n_d \leqslant p \\ n_1 + n_2 + \ldots + n_d \leqslant p + 1 \\ n_1 + a_2 n_2 + \ldots + a_d n_d \equiv i \bmod p \end{array} \right\} - \# \left\{ \begin{array}{l} 0 \leqslant n_1, n_2, \ldots, n_d \leqslant p \\ n_1 + n_2 + \ldots + n_d \leqslant p \\ n_1 + a_2 n_2 + \ldots + a_d n_d \equiv i \bmod p \end{array} \right\}.$$

Quand on enlève l'intersection de ces deux simplexes, on obtient

$$F_{i-1}(\mathbf{a}, p) - F_i(\mathbf{a}, p) = \# \left\{ \begin{array}{l} 1 \leqslant n_1 \leqslant p + 1 \\ 0 \leqslant n_2, \ldots, n_d \leqslant p \\ n_1 + n_2 + \ldots + n_d = p + 1 \\ n_1 + a_2 n_2 + \ldots + a_d n_d \equiv i \bmod p \end{array} \right\} - \# \left\{ \begin{array}{l} 0 \leqslant n_2, \ldots, n_d \leqslant p \\ n_2 + \ldots + n_d \leqslant p \\ a_2 n_2 + \ldots + a_d n_d \equiv i \bmod p \end{array} \right\}.$$

D'où, par l'hypothèse de récurrence,

$$F_{i-1}(\mathbf{a}, p) - F_i(\mathbf{a}, p) = \left\{ \begin{array}{ll} -1 & \text{if } i = 0 \\ +1 & \text{if } i = 1 \\ 0 & \text{sinon.} \end{array} \right.$$

ce qui équivaut à (2.60). □

L'idée de cette preuve peut être utilisée pour montrer la Proposition 2.2.2. D'après la Proposition 2.6.1, on a

$$F_1(\mathbf{a},p)=\frac{\binom{d}{d+p}-1}{p} \text{ et } F_0(\mathbf{a},p)=\frac{\binom{d}{d+p}+p-1}{p} \tag{2.61}$$

On peut formuler le problème suivant :

Problème 4 (Le problème inverse des triangles de Pascal)**.** *Soient p un nombre premier et d un entier tels que $p>d\geqslant 0$. Décrire toutes les fonctions*

$$\triangle:(\mathbb{N}\cup\{-1\})^d\to\mathbb{Z}$$

telles que

$$n_1+n_2+\ldots+n_d\geqslant p\Rightarrow\triangle(n_1,n_2,\ldots,n_d)=0; \tag{2.62}$$

$$\exists i,\ n_i<0\Rightarrow\triangle(n_1,n_2,\ldots,n_d)=0; \tag{2.63}$$

$$\triangle(0,0,\ldots,0)=1; \tag{2.64}$$

$$\forall(n_1,\ldots,n_d)\in\mathbb{N}^d\setminus\mathcal{S}_0\setminus\mathcal{S},\ \triangle(n_1,n_2,\ldots,n_d)=\sum_i\triangle(n_1,\ldots,n_{i-1},n_i-1,n_{i+1},\ldots,n_d). \tag{2.65}$$

où $\mathcal{S}_0=\{(0,\ldots,0),(p,0,\ldots,0),\ldots,(0,0,\ldots,p)\}$ et $\mathcal{S}$ est un ensemble dont tous les éléments ont au moins deux coordonnées non nulles, de taille $|\mathcal{S}|\leqslant\frac{\binom{d}{d+p}-dp-1}{p}$. Répondre s'il existe un exemple où cette inégalité est stricte.

Les éléments de $\mathcal{S}_0$ seront appelés les *sources triviales,* car d'après les conditions du problème, l'équation (2.65) ne peut pas y être réalisée. On a en fait pour tout point d'une arête du simplexe dont une des extrémités se trouve au sommet $(0,0,\ldots,0)$ (c'est à dire pour tout point de la forme $X=(0,\ldots,0,n,\ldots,0)$ où $0<n<p$) l'identité $\triangle(X)=+1$.

Ajoutons deux autres remarques générales : pour tout d-uplet de résidus $(a_1,\ldots,a_d)$ différents et non nuls, la fonction

$$(-1)^{n_1+\ldots+n_d}(A_1(f_{n_{a_1}=n_1,\ldots,n_{a_d}=n_d},p)-A_0(f_{n_{a_1}=n_1,\ldots,n_{a_d}=n_d},p))$$

est une solution du Problème 4; on appellera ces solutions *les solutions induites par la combinatoire modulo p.* D'autre part (comparer à la remarque au début du chapitre 2.5), le fait de remplacer l'équation (2.65) par une autre équation linéaire à coefficients non nuls mène à un problème équivalent.

Introduisons une définition auxiliaire qui justifie le terme "source". En tout point $\mathbf{x}\in\mathbb{N}^d$ appelons la *puissance* de ce point (en tant que source) le nombre

$$f(\mathbf{x})=\triangle(\mathbf{x})-\sum_{i=1}^{d}\triangle(\mathbf{x}-\mathbf{e}_i) \tag{2.66}$$

où $\mathbf{e}_i$ sont les vecteurs $(0,\ldots,0,1,0,\ldots,0)$ avec la coordonnée 1 à la i-ème position). D'après la linéarité de l'équation (2.65), on a

$$\triangle(n_1,\ldots,n_d)=\sum_{(m_1,\ldots,m_d)\leqslant(n_1,\ldots,n_d)}f(m_1,\ldots,m_d)\binom{n_1+n_2+\ldots+n_d-m_1-m_2-\ldots-m_d}{n_1-m_1,n_2-m_2,\ldots,n_{p-1}-m_{p-1}}, \tag{2.67}$$

où la relation d'ordre entre les d-uplets d'entiers est l'ordre terme par terme.

La deuxième partie du Problème 4 restera en état de conjecture même en cas de deux dimensions, auquel on va se restreindre, et pour lequel on proposera une piste de solution.

Dans le cas des solutions induites par la combinatoire modulo p, les puissances de toutes les sources non triviales sont multiples de p. On peut maintenant montrer ce résultat dans un cas plus général.

Théorème 2.6.2. *Dans le cadre du Problème 4, supposons $d = 2$ et remplaçons l'hypothèse sur la borne de $|\mathcal{S}|$ par l'hypothèse suivante : $\mathcal{S}$ ne contient pas plus d'un point de chaque abscisse fixe (entre 1 et $p-1$). Alors, les puissances de toutes les sources non triviales sont multiples de p.*

Démonstration. Supposons que les sources non triviales sont situées dans les points $(1, k_1), (2, k_2), (3, k_3) \ldots$, et leurs puissances respectives sont égales à $f_1, f_2, \ldots$ La nouvelle hypothèse permet d'exprimer les puissannces par un procédé analogue à celui décrit dans la partie 2.4. En effet, en ajoutant les équations (2.66) aux points $(1, n)$, on obtient

$$f_1 = -\sum_{n=0}^{p-1} \triangle(0, n). \tag{2.68}$$

En ajoutant ces équations aux points $(2, n)$, on obtient

$$f_2 = -\sum_{n=0}^{p-2} \triangle(1, n). \tag{2.69}$$

En général pour tout $l \in \{1, \ldots, p-1\}$,

$$f_l = -\sum_{n=0}^{p-l} \triangle(l-1, n). \tag{2.70}$$

Montrons le Théorème par récurrence sur l'abscisse l de la source. D'après (2.68), on a $f_1 = -p$.

Le pas de récurrence se fait de façon suivante : supposons que $f_1, f_2, \ldots, f_{l-1}$ sont multiples de p. Alors, d'après (2.67), pour chaque point (n_1, n_2) tel que $n_1 < l$, on a : $\triangle(n_1, n_2) \equiv \binom{n_1}{n_1+n_2} \bmod p$. Par conséquent,

$$f_l = -\sum_{n=0}^{p-l} \triangle(l-1, n) \equiv -\sum_{n=0}^{p-l} \binom{l-1}{n+l-1} = -\binom{l}{p} \equiv 0 \bmod p.$$

□

Les formules (2.67) et (2.68), appliquées récursivement, permettent aussi de déterminer la fonction $\triangle$ à partir de la donnée de $\mathcal{S}$.

Par contre, il existe des solutions du Problème 4 qui ne vérifient pas l'hypothèse du Théorème 2.6.2. Voici le plus petit exemple (pour $p = 7$) :

$$\begin{array}{ccccccccccc}
 & & & & +1 & & & & & & \\
 & & & +1 & & +1 & & & & & \\
 & & +1 & & +2 & & +1 & & & & \\
 & +1 & & +3 & & +3 & & +1 & & & \\
 +1 & & -3_{\blacklozenge} & & +6 & & -3_{\blacklozenge} & & +1 & & \\
 & +1 & & -2 & & +3 & & -2 & & +1 & \\
+1 & & -1 & & +1 & & -1_{\blacklozenge} & & +1 & & -1 & & +1
\end{array}$$

Terminons ce chapitre par l'étude d'un énoncé algébrique équivalent (en 2 dimensions) au problème inverse des triangles de Pascal. On peut faire correspondre une solution du problème à un ensemble de sources non triviales (n_k, m_k) avec des puissances f_k tel que la fonction $\triangle$ définie par (2.67) vérifie pour chaque

$n \in \{0, p\} : \triangle(n, p-n) = 0$. La suite $(\triangle(n, p-n))_n$ se décompose en une somme des influences de différentes sources, où les influences des sources triviales sont prescrites et leur somme vaut

$$(0, p, \binom{2}{p}, \binom{3}{p}, \ldots, p, 0);$$

l'influence de chaque source non triviale est une ligne du triangle de Pascal classique, décalée de façon appropriée, complétée par des zéros, et multipliée par la puissance f_k. Si on associe à chaque suite d'entiers le polynôme dont cette suite est la suite des coefficients, on arrive à la formulation suivante :

Problème 5 (équivalent au problème inverse des triangles de Pascal en 2 dimensions)**.** *Soit p un nombre premier impair. Décrire l'ensemble des solutions de l'équation*

$$(X+1)^p - X^p - 1 = \sum_{i=1}^{\frac{p-1}{2}} f_i X^{x_i} (X+1)^{y_i} \tag{2.71}$$

dans $\mathbb{Z}[X]$ avec $x_i, y_i \in \{1, \ldots, p-2\}$. Répondre si une solution avec une somme de $\frac{p-3}{2}$ termes existe.

Par exemple, le triangle de Pascal de taille $p = 7$ ci-dessus correspond à la solution

$$(X+1)^7 - X^7 - 1 = 7X(X+1)^3 + 7X^3(X+1)^3 + 7X^2(X+1).$$

Pour $p = 7$, il existe cinq autres solutions qui sont

$$\begin{aligned}(X+1)^7 - X^7 - 1 &= 7X^3(X+1)^3 + 14X^2(X+1)^2 + X(X+1),\\ (X+1)^7 - X^7 - 1 &= 7X^2(X+1)^4 - 7X^4(X+1) + 7X(X+1)^2,\\ (X+1)^7 - X^7 - 1 &= 7X(X+1)^5 - 14X^2(X+1)^3 + 7X^3(X+1)\end{aligned}$$

et les réciproques des deux premières ; ces solutions sont induites par la combinatoire modulo 7.

Comme le terme de droite de (2.71) est défini à un facteur scalaire près, il est naturel d'étudier la factorisation du polynôme $P_p(X) = (X+1)^p - X^p - 1$. Formulons quelques remarques simples (valables pour tout p congru à 1 ou 5 modulo 6 sans exiger que p soit premier) : P_p est un polynôme de degré $p-1$, qui compte parmi ses racines $0, -1, e^{\frac{2i\pi}{3}}$ et $e^{-\frac{2i\pi}{3}}$ (toutes ces racines sont simples si $p \equiv 5 \bmod 6$, sinon $e^{\frac{2i\pi}{3}}$ et $e^{-\frac{2i\pi}{3}}$ sont des racines doubles), et dont les racines sont conservées par les transformations $z \to \bar{z}, z \to -1-z$ (la symétrie par rapport au point $-\frac{1}{2}$) et $z \to \frac{1}{z}$ (car le polynôme est réciproque). La description complète des positions des racines de $P_p(X)$ fait l'objet du théorème suivant :

Théorème 2.6.3. *Soit n un entier congru à 1 ou à 5 modulo 6, $n \geqslant 5$. Alors toutes les racines de $P_n(X) = (X+1)^p - X^p - 1$ se trouvent sur la réunion des lignes suivantes (qui a une forme de lentille) :*

la droite $-1/2 + i\mathbb{R}$ privée de l'intervalle ouvert $]e^{-\frac{2i\pi}{3}}, e^{\frac{2i\pi}{3}}[$;

les deux arcs de cercles de $e^{\frac{2i\pi}{3}}$ jusqu'à $e^{-\frac{2i\pi}{3}}$ centrés en 0 et en -1 .

L'Annexe 5 montre l'ensemble de ces racines pour $n = 25$ ainsi que la réunion de toutes les racines (de partie imaginaire inférieure à 1 en valeur absolue) pour les nombres premiers n compris entre 11 et 97. Ces dessins suggèrent une équidistribution des racines sur les arcs de cercles, qui est formalisée dans la preuve.

Démonstration. Commençons par le cas $n \equiv 5 \bmod 6$, et montrons que $\frac{n-5}{6}$ racines sont situées sur l'arc de cercle $]e^{\frac{2i\pi}{3}}, -1[$ centré en 0. Par symétrie de la position des racines, cela montrera qu'autant de racines se trouvent sur chacun des trois arcs $]-1, e^{-\frac{2i\pi}{3}}[,]e^{-\frac{2i\pi}{3}}, 0[$ et $]0, e^{\frac{2i\pi}{3}}[$, et sur chacune des demi-droites ; cela suffit donc pour localiser toutes les racines de P_n.

Posons $x = e^{i\theta}$ et faisons varier θ de $\frac{2\pi}{3}$ jusqu'à π. Alors, le point $Z(\theta) = -x^n$ varie de $e^{\frac{i\pi}{3}}$ jusqu'à 1 en faisant $\frac{n+1}{6}$ tours de cercle (dont le premier est incomplet). D'après le fait que $|(x+1)^n| < 1$ quand $\theta > \frac{2\pi}{3}$, le

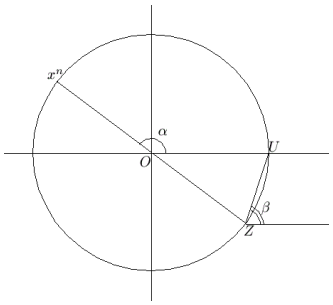


FIGURE 2.2. $\beta = \frac{\alpha}{2}$

point $D(\theta) = (x+1)^n - x^n$ varie de 1 jusqu'à 1 en faisant aussi $\frac{n+1}{6}$ tours autour de l'origine. Notre objectif consiste donc à montrer que près de chaque instant où $Z(\theta) = 1$ se trouve un instant θ' où $D(\theta') = 1$.

Commençons par remarquer qu'un argument de $x+1$ est $\frac{\theta}{2}$. Ensuite, on montre par la géométrie élémentaire que les points Z, D et 1 sont toujours alignés. Cet argument est illustré par le dessin Figure 2.2, où le point Z se trouve entre $-i$ et 1 (les autres configurations sont analogues).

On a $\beta = \angle ZUO$ (on appelle O le point d'affixe 0 et U le point d'affixe 1 pour respecter le style des notations géométriques), car les droites sont parallèles, et $\angle ZUO = \frac{\alpha}{2}$, car c'est un angle d'un triangle isocèle. Comme l'angle β et l'argument de $(x+1)^n$ diffèrent d'un multiple de π, les points Z, D, U sont alignés.

Tournons-nous maintenant vers la question de la position respective de ces trois points sur la droite, plus précisément vers le signe du produit scalaire $\overrightarrow{ZD}.\overrightarrow{ZU}$. Il est clair que ce signe change exactement aux moments où $Z(\theta) = U$.

Maintenant, on peut montrer ce qui a été annoncé plus haut : près de chaque instant de passage du point Z par U se trouve un instant de passage du point D par U. Précisément, supposons que $\theta_1 \in]\frac{2\pi}{3}, \frac{\pi}{2}[$ est un instant tel que $Z(\theta_1) = U$. Soit $\theta_0 = \theta_1 - \frac{\pi}{2n} = \max\{\theta < \theta_1 | Z(\theta_0) = -i\}$ et $\theta_2 = \theta_1 + \frac{\pi}{2n} = \min\{\theta > \theta_1 | Z(\theta_2) = i\}$. On va montrer qu'il existe $\theta \in]\theta_0, \theta_2[$ tel que $D(\theta) = U$. Si $\overrightarrow{Z(\theta_0)D(\theta_0)}.\overrightarrow{Z(\theta_0)U} > 0$, la même chose vaut dans tout l'intervalle $[\theta_0, \theta_1[$. On a $|Z(\theta_0)D(\theta_0)| < \sqrt{2} = |Z(\theta_0)U|$ et $|Z(\theta_1)D(\theta_1)| > 0 = |Z(\theta_1)U|$, d'où (par continuité de ces fonctions) il existe un instant $\theta' \in]\theta_0, \theta_1[$ tel que $|Z(\theta')D(\theta')| = |Z(\theta')U|$, d'où $D(\theta') = U$. Maintenant, si $\overrightarrow{Z(\theta_0)D(\theta_0)}.\overrightarrow{Z(\theta_0)U} < 0$, alors $\overrightarrow{Z(\theta)D(\theta)}.\overrightarrow{Z(\theta)U} > 0$ pour tout $\theta \in]\theta_1, \theta_2]$; on trouve donc dans cet intervalle un instant θ' tel que $|Z(\theta')D(\theta')| = |Z(\theta')U|$, d'où $D(\theta') = U$.

Le cas où $n \equiv 1 \bmod 6$ est analogue. Quand $\theta = \arg x$ varie de $\frac{2\pi}{3}$ jusqu'à π, le point $-x^n$ varie de $e^{\frac{5\pi}{6}}$ jusqu'à 1 en parcourant un arc de longueur $\frac{\pi}{6}$ puis $\frac{n-1}{6}$ tours de cercle complets. Près (au même sens que précédemment) de chaque instant $\theta_1 \in]\frac{2\pi}{3} + \frac{\pi}{n}, \frac{\pi}{2}[$ tel que $Z(\theta_1) = -e^{in\theta_1} = 1$, se trouve un instant θ tel que $D(\theta) = 1$, ce qui montre que le polynôme $P_n(x)$ a au moins $\frac{n-7}{6}$ racines sur l'arc de cercle $]e^{\frac{2i\pi}{3}}, -1[$ centré en 0. □

Chapitre 3

Annexes

3.1 Les lignes fractales de raréfaction pour $p = 3, 5$

Les figures suivantes illustrent la raréfaction de pas 3 et 5 pour la suite de Thue-Morse, et la raréfaction de pas 3 pour la suite de Thue-Morse en base (-2). La figure 3.1 represente le tracé (sous forme d'une suite de segments) des 4^5 premières sommes partielles de la suite 4-multiplicative qui commence par $(1, e^{\frac{5i\pi}{3}}, e^{\frac{i\pi}{3}}, 1, \ldots)$, elle peut être vue comme un tracé approximatif du graphe de la fonction $\psi(x)$ correspondante, qui n'est rien d'autre que le flocon de Koch. La figure 3.3 représente les 16^2 premières sommes partielles de la somme $\sum_{n=0}^{N} t_n \zeta^n$, où (t_n) est la suite de Thue-Morse et $\zeta = e^{\frac{2i\pi}{5}}$. Les figures 3.5, 3.6 et 3.7 sont des tracés des sommes partielles de la même somme $\sum_{n=0}^{N} \tau_n$ où (τ_n) est la suite $4_{<-2>}$-multiplicative définie dans le chapitre 1.3 par $\tau_0 = 1, \tau_1 = -j, \tau_{-2} = -j, \tau{-}1 = j^2$; le nombre de segments dans ces figures vaut respectivement 22, 342 et 1366.

La figure 3.2 est le nuage des points d'ordonnée

$$N^{-\log_4 3} \sum_{\substack{n < N \\ 3|n}} t_n$$

et d'abscisse $\{\log_4(N)\}$, où N varie de 2 jusqu'à 10000 et (t_n) est la suite de Thue-Morse ; ces points convergent vers le graphe de la fonction F du théorème 0.0.3. La figure 3.4 est le nuage des points d'ordonnée

$$N^{-\log_{16} 5} \sum_{\substack{n < N \\ 5|n}} t_n$$

et d'abscisse $\{\log_4(N)\}$ où N varie de 2 jusqu'à 50000 et t_n est la suite de Thue-Morse.

Les graphes sur les figures $4.1 - 4$ ont déjà été publiés.

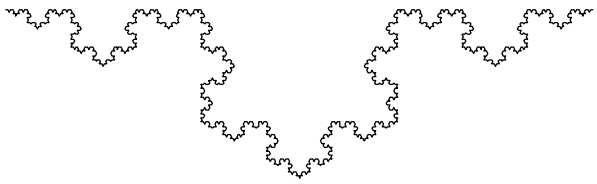


FIGURE 3.1 – Le flocon de Koch.

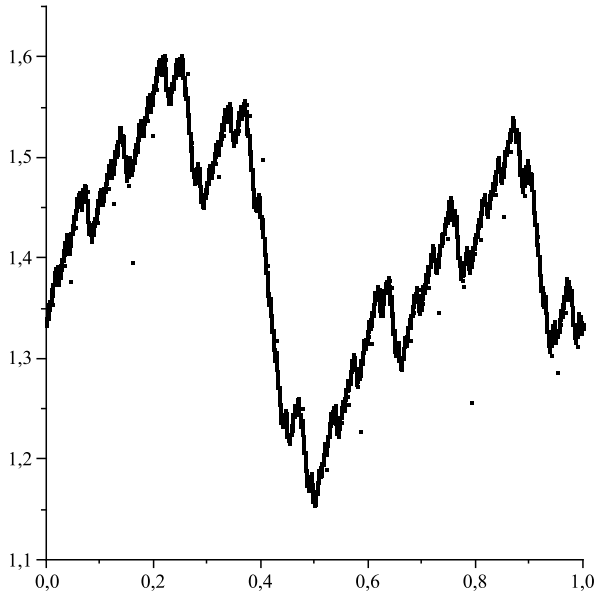


FIGURE 3.2 – $S_{3,0}(3N)/N^{\alpha_3}$ en fonction de $\{\log_4(N)\}$ quand N varie de 2 à 10000.

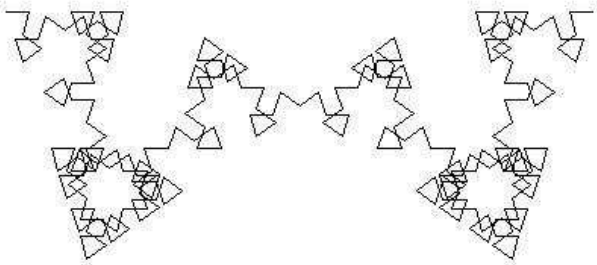


FIGURE 3.3 – $\zeta = e^{\frac{2 \cdot 2i\pi}{5}}$: deux premières itérations.

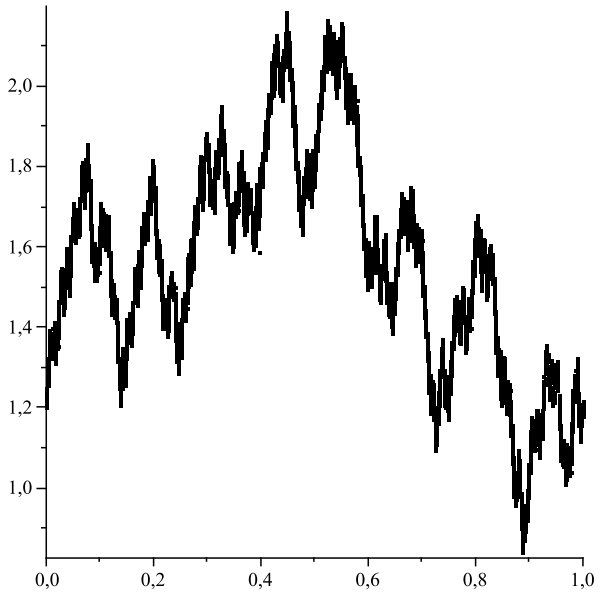


FIGURE 3.4 – $S_{5,0}(5N)/N^{\alpha_5}$ en fonction de $\{\log_{16}(N)\}$ quand N varie de 2 à 50000.

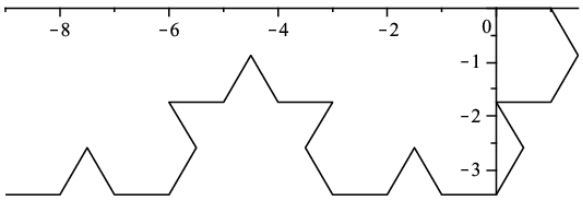


FIGURE 3.5 – Le flocon de Koch associé à la base (-2) : 22 premiers segments.

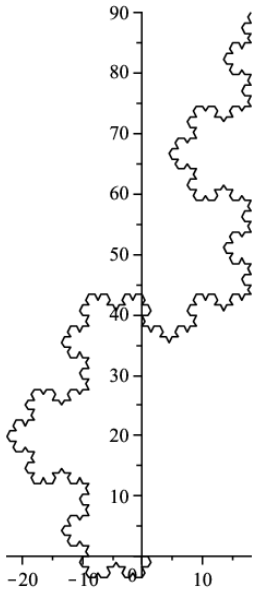


FIGURE 3.6 – Le flocon de Koch associé à la base (-2) : 342 premiers segments.

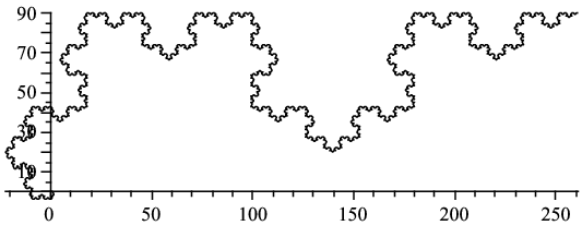


FIGURE 3.7 – Le flocon de Koch associé à la base (-2) : 1366 premiers segments.

3.2 La première étape d'itération pour p plus élevé

Les figures suivantes représentent les $2^{s(p)}$ premières sommes partielles de la somme $\sum_{n=0}^{N} t_n \zeta^n$ où $p \geqslant 5$ est premier, s est l'ordre de 2 dans le groupe $\mathbb{F}_p^\times$, (t_n) est la suite de Thue-Morse et ζ est une racine primitive p-ième de l'unité. L'inscription sous chaque dessin indique la valeur de p et la racine ζ choisie. Les figures 3.14 et 3.15 méritent une remarque particulière : elles représentent le même objet mathématique, mais à différentes échelles. Les figures 3.8 et 3.10 ont déjà été publliées dans [8], mais les moyens techniques de l'époque ne permettaient pas de produire celles à partir de 3.11.

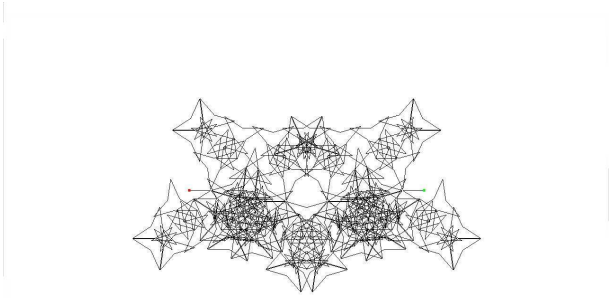


FIGURE 3.8 – $\zeta = e^{\frac{2i\pi}{11}}$.

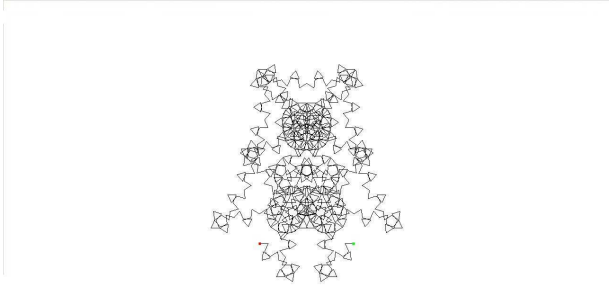


FIGURE 3.9 – $\zeta = e^{\frac{2\cdot 2i\pi}{11}}$.

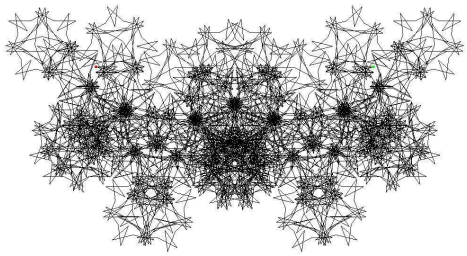


FIGURE 3.10 – $\zeta = e^{\frac{2i\pi}{13}}$.

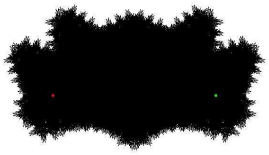


FIGURE 3.11 – $\zeta = e^{\frac{2i\pi}{19}}$.

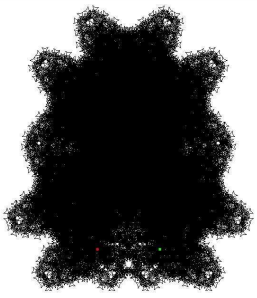


FIGURE 3.12 – $\zeta = e^{\frac{2\cdot 2i\pi}{19}}$.

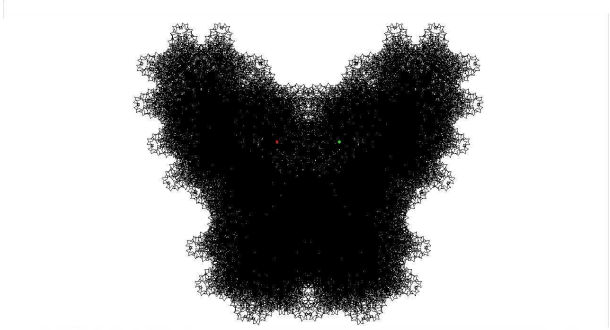


FIGURE 3.13 – $\zeta = e^{\frac{3 \cdot 2i\pi}{19}}$.

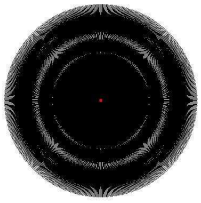


FIGURE 3.14 – $\zeta = e^{\frac{2i\pi}{241}}$.

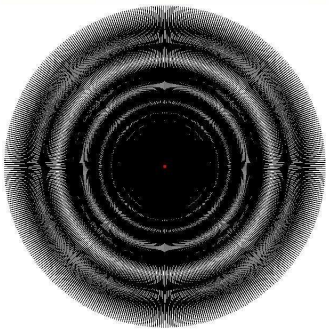


FIGURE 3.15 – $\zeta = e^{\frac{2i\pi}{241}}$.

3.3 Le code source de la suite de Thue-Morse

Les fragments de code suivants (en assembleur inline) calculent une valeur de la suite de Thue-Morse. L'interface avec le programme en C est la suivante : l'entrée est composée d'une variable n de type `unsigned int` et d'une variable *thueMorse* de type `int`, à la sortie *thueMorse* prend la valeur

$$t_n = (-1)^{\text{le numbre de chiffres } '1' \text{ dans l'écriture binaire de } n}.$$

Le code suivant est écrit en syntaxe AT&T et peut être compilé par `gcc`.

```
asm("movl $1, %0;"
"cmpl $0, %1;"
"jnp _byte2;"
"negl %0;"
"_byte2:;"
" roll $8,%1;"
" cmpl $0, %1;"
" jnp _byte3;"
" negl %0;"
```

```
"_byte3:;"
" roll $8,%1;"
" cmpl $0, %1;"
" jnp _byte4;"
" negl %0;"
"_byte4:;"
" roll $8,%1;"
" cmpl $0, %1;"
" jnp _fini;"
" negl %0;"
"_fini:;"
"roll $8,%1;"
:"=&r"(thueMorse)
:"r"(n)
);
```

Les utilisateurs de Visual C++ auront bésoin de la variante suivante (écrite en syntaxe INTEL) :

```
__asm{push eax
push ebx
mov ebx, n

mov eax, 1
cmp ebx, 0
jnp _byte2
neg eax
_byte2:
rol ebx,8
cmp  ebx,0
jnp _byte3
neg eax
_byte3:
rol ebx, 8
cmp ebx, 0
jnp _byte4
neg eax
_byte4:
rol ebx, 8
cmp ebx, 0
jnp _fini
neg eax
_fini:

mov thueMorse, eax
pop ebx
pop eax
};
```

3.4 Le tétraèdre de Pascal pour $p = 11, \mathcal{I} = \{1, 2, 3\}$

Les tableaux suivants forment le tétraèdre de Pascal de taille $p = 11$ associé à $\mathcal{I} = \{1, 2, 3\}$. Ce sont les intersections du tétraèdre avec les plans parallèles définis par une valeur de la coordonnée n_0. L'origine du système des coordonnées décrit dans le chapitre 2.4 est le premier "triangle" d'un point, l'axe des n_1 traverse les sommets supérieurs des triangles, l'axe des n_2 traverse les sommets inférieur-gauches et l'axe des n_3 traverse les sommets inférieur-droits. Les cercles indiquent les sources (situées dans deux plans parallèles d'équations $n_1 + 2n_2 + 3n_3 = 11$ et $n_1 + 2n_2 + 3n_3 = 22$), et les losanges se trouvent au-dessus les sources extérieures. Remarquons que le fait de voir l'équation de Pascal du tétraèdre demande un peu d'habitude car cette équation relie la valeur en un point avec trois valeurs situées dans le plan au-dessus.

La face de fond (d'équation "$n_0 = 0$") est identique au triangle de Pascal de taille $p = 11$ qui correspond à $\mathcal{I} = \{1, 2\}$. Après l'identification l'origine du nouveau repère est le sommet de haut, le nouvel axe des n_1 est le côté gauche, et le nouvel axe des n_2 est le côté droit. Les sources relatives à ce triangle sont indiquées par les losanges.

$\underline{n_0 = 10}$	$\underline{n_0 = 9}$	$\underline{n_0 = 8}$	$\underline{n_0 = 7}$
$+1$	-1 $-1 \quad -1$	$+1$ $+2 \quad +2$ $+1 \quad +2 \quad +1$	-1 $-3 \quad -3$ $-3 \quad -6 \quad -3$ $-1 \quad -3 \quad -3 \quad -1$

$\underline{n_0 = 6}$

$$
\begin{array}{ccccccc}
 & & & +1 & & & \\
 & & +4 & & +4 & & \\
 & +6 & & +12 & & +6 & \\
+4 & & +12 & & +12 & & +4 \\
+1 & & +4 & & +6 & & -7_\circ \quad +1
\end{array}
$$

$\underline{n_0 = 5}$

$$
\begin{array}{ccccccccc}
 & & & & -1 & & & & \\
 & & & -5 & & -5 & & & \\
 & & -10 & & -20 & & -10 & & \\
 & -10 & & -30 & & -30 & & +12_\circ & \\
-5 & & -20 & & +36_\circ & & -9 & & -5 \\
-1 & & +6_\circ & & -10 & & +1 & & +6 \quad -1
\end{array}
$$

$\underline{n_0 = 4}$

$$
\begin{array}{ccccccccc}
 & & & & +1 & & & & \\
 & & & +6 & & +6 & & & \\
 & & +15 & & +30 & & +15 & & \\
 & +20 & & +60 & & -50_\circ & & -2 & \\
+15 & & -50_\circ & & +24 & & +27 & & +7 \\
+5_\circ & & +19 & & -6 & & -28 & +8 & -6 \\
+1 & & -5 & & +4 & & +9 & -7 \quad -5 & +1
\end{array}
$$

$\underline{n_0 = 3}$

$$
\begin{array}{ccccccccccc}
 & & & & & -1 & & & & & \\
 & & & & -7 & & -7 & & & & \\
 & & & -21 & & -42 & & +12_\circ & & & \\
 & & -35 & & +60_\circ & & +5 & & -13 & & \\
 & +20_\circ & & -30 & & -34 & & +25 & & +9 & \\
-10 & & +16 & & +32 & & -23 & & -28 & & +1 \\
+4 & & -9 & & -17 & & +25 & & +27 & -9 \quad -7 & \\
-1 & +4 & & +1 & & -13 & & +2 & & +12 \quad +4 \quad -1 &
\end{array}
$$

$\underline{n_0 = 2}$

$$
\begin{array}{ccccccccccccccc}
 & & & & & & +1 & & & & & & & & \\
 & & & & & +8 & & +8 & & & & & & & \\
 & & & & +28 & & -21_\circ & & -5 & & & & & & \\
 & & & -21_\circ & & +3 & & +25 & & +1 & & & & & \\
 & & +15 & & +5 & & -31 & & -17 & & +4 & & & & \\
 & -10 & & -6 & & +32 & & +32 & & -6 & & -10 & & & \\
 +6 & & +3 & & -31 & & -34 & & +24 & & +36 & & +6 & & \\
 -3 & & +1 & & +25 & & +5 & & -50 & & -30 & & +12 & & -3_\circ \\
 +1 & & -3 & & -5 & & +12 & & +15 & & -10 & & +6_\circ & & -3 & & +1
\end{array}
$$

$\underline{n_0 = 1}$

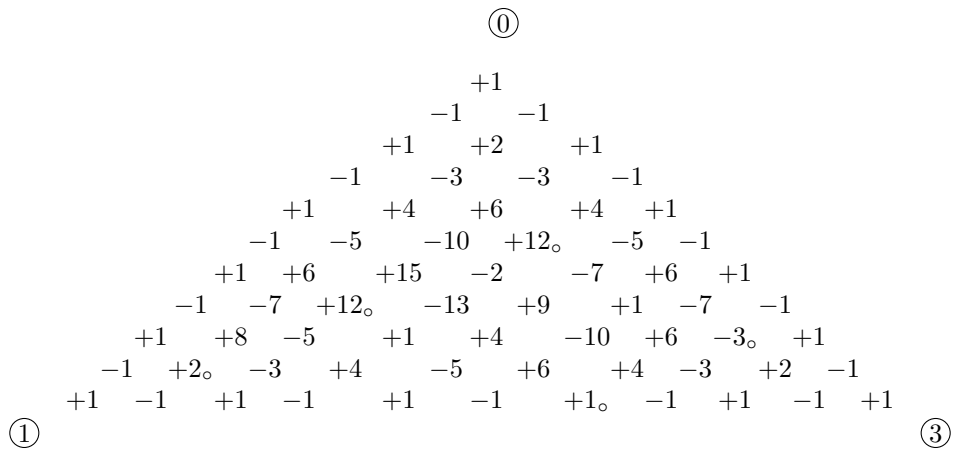
$$
\begin{array}{ccccccccccccccc}
 & & & & & & -1 & & & & & & & & \\
 & & & & & -9 & & +2_\circ & & & & & & & \\
 & & & & +8_\circ & & +5 & & -3 & & & & & & \\
 & & & -7 & & -10 & & +1 & & +4 & & & & & \\
 & & +6 & & +13 & & +3 & & -9 & & -5 & & & & \\
 & -5 & & -14 & & -6 & & +16 & & +19 & & +6 & & & \\
 +4 & & +13 & & +5 & & -30 & & -50 & & -20 & & +4 & & \\
 -3 & & -10 & & +3 & & +60 & & +60 & & -30 & & +12_\circ & & -3 \\
 +2 & & +5 & & -21 & & -42 & & +30 & & -20_\circ & & +12 & & -6 & & +2 \\
 +1 & & +2 & & +8 & & -7 & & +6_\circ & & -5 & & +4 & & -3 & & +2 & & -1
\end{array}
$$

$\underline{n_0 = 0}$

$$
\begin{array}{ccccccccccccccc}
 & & & & & & \otimes & \text{axe des } n_1 & & & & & & & \\
 & & & & & & +1 & & & & & & & & \\
 & & & & & -1_\circ & & -1 & & & & & & & \\
 & & & & +1 & & +2 & & +1 & & & & & & \\
 & & & -1 & & -3 & & -3 & & -1 & & & & & \\
 & & +1 & & +4 & & +6 & & +4 & & +1 & & & & \\
 & -1 & & -5 & & -10 & & -10 & & -5 & & -1 & & & \\
 +1 & & +6 & & +15 & & +20 & & +15 & & -5_\blacklozenge & & +1_\circ & & \\
 -1 & & -7 & & -21 & & -35 & & +20_\blacklozenge & & -10_\circ & & +4 & & -1 \\
 +1 & & +8 & & +28 & & -21_\blacklozenge & & +15_\circ & & -10 & & +6 & & -3 & & +1 \\
 -1 & & -9 & & +8_\blacklozenge & & -7_\circ & & +6 & & -5 & & +4 & & -3 & & +2 & & -1 \\
 +1 & & -1_\blacklozenge & & +1_\circ & & -1 & & +1 & & -1 & & +1 & & -1 & & +1 & & -1 & & +1
\end{array}
$$

axe des $n_2\otimes$ $\otimes$axe des n_3

Le triangle suivant est la face du tétraèdre précédent, composée des côtés droits des tableaux triangulaires ci-dessus, qui coincide avec le triangle de Pascal qui correspond à $\mathcal{I} = \{1, 3\}$.


⓪
+1
−1 −1
+1 +2 +1
−1 −3 −3 −1
+1 +4 +6 +4 +1
−1 −5 −10 +12∘ −5 −1
+1 +6 +15 −2 −7 +6 +1
−1 −7 +12∘ −13 +9 +1 −7 −1
+1 +8 −5 +1 +4 −10 +6 −3∘ +1
−1 +2∘ −3 +4 −5 +6 +4 −3 +2 −1
+1 −1 +1 −1 +1 −1 +1∘ −1 +1 −1 +1
① ③

3.5 Les racines de $(X+1)^{25} - X^{25} - 1$

Le graphique suivant montre la position des racines du polynôme $(X+1)^{25} - X^{25} - 1$.

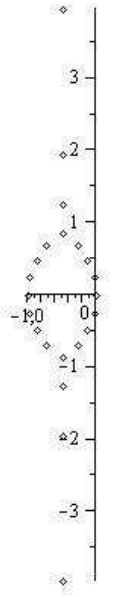


FIGURE 3.16 – Les racines de $(X+1)^{25} - X^{25} - 1$.

Le graphique suivant montre la position des racines des polynômes $(X+1)^p - X^p - 1$ de parties imaginaires comprises entre -1 et 1, où p parcourt tous les nombres premiers entre 11 et 97.

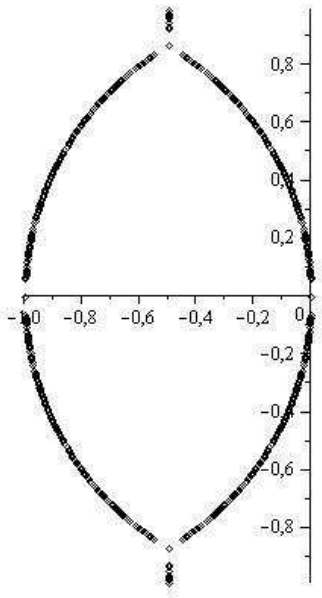


FIGURE 3.17 – Les racines de $(X+1)^p - X^p - 1$ $(11 \leqslant p \leqslant 97)$.

3.6 Le lien entre l'automaticité et la condition de finitude

Dans cette sous-section, on va établir le rapport entre la notion de suite b-multiplicative vérifiant la condition de finitude, utilisée tout le long du texte, et la notion de suite b-multiplicative et b-automatique. Une suite b-automatique est nécessairement restreinte à un ensemble fini de valeurs. Comme mentionné dans l'Introduction, il est facile de montrer qu'une suite b-multiplicative vérifiant la condition de finitude et à valeurs dans un ensemble fini, est b-automatique; de plus, ses valeurs sont comprises dans l'union de zéro et des racines de l'unité. Nous allons montrer ici la correspondance au sens réciproque.

Proposition 3.6.1. *Soit (t_n) une suite b-multiplicative et b-automatique. Alors, il existe $R, h \in \mathbb{N}, R > 0$ et une suite b^R-multiplicative $\bar{t}$ qui vérifie la condition de finitude tels que*

$$t_n = \bar{t}_{[\frac{n}{b^h}]} \cdot t_{n-b^h[\frac{n}{b^h}]}. \tag{3.1}$$

Démonstration. Comme la suite (t_n) est b-multiplicative, il existe une fonction

$$\check{t} : \mathbb{N} \times \{0, 1, \ldots, b-1\} \to \mathbb{C}$$

telle que

$$t_{\overline{c_l c_{l-1} \ldots c_0}} = \prod_{i=0}^{l} \check{t}(i, c_i).$$

Définissons pour chaque $i \in \mathbb{N}$ la fonction $\check{t}_i$ par $\check{t}_i(c) = \check{t}(i, c)$. Supposons que la suite (t_n) n'est nulle à partir d'aucun rang.

Soit $A =< \{0,1,\ldots,b-1\}, Q, \delta, q_0, \tilde{t} >$ un automate fini déterministe qui reconnait la suite (t_n) ; son alphabet est $\{0,1,\ldots,b-1\}$; Q est son ensemble d'états ; $\delta : Q \times \{0,1,\ldots,b-1\} \to Q$ est sa fonction de transition ; $q_0 \in Q$ est l'état initial ; $\tilde{t} : Q \to \mathbb{C}$ est la fonction réponse, $t_{\overline{c_l c_{l-1} \ldots c_0}}$ sera toujours égal à $\tilde{t}$ évaluée dans l'état résultant de l'execution de l'automate sur le mot $c_l c_{l-1} \ldots c_0$. Pour préciser les notations, supposons que l'automate lit le mot d'entrée de droite à gauche. Notons $Q^0 = \tilde{t}^{-1}(\{0\})$, c'est un "sous-ensemble puits" au sens où si $q \in Q^0$, alors pour chaque chiffre c, on a $\delta(q,c) \in Q^0$. Définissons la fonction $\bar{\delta} : \mathfrak{P}(Q) \to \mathfrak{P}(Q)$ par $\bar{\delta}(X) = \{q \in Q | \exists x \in X \exists c \in \{0,1,\ldots,b-1\}\ \delta(x,c) = q\}$. Comme Q est fini, la suite $(\bar{\delta}^k(\{q_0\}))_k$ est ultimement périodique, ainsi que la suite $(\bar{\delta}^k(\{q_0\}) \setminus Q^0)_k$ (d'après l'hypothèse, tous les termes de cette dernière suite sont non vides).

Si, pour deux entiers naturels k et l, $\bar{\delta}^k(\{q_0\}) \cap \bar{\delta}^l(\{q_0\}) \setminus Q^0 \neq \emptyset$, alors $\check{t}_k = \check{t}_l$, d'où la suite $(\check{t}_k)_k$ est aussi ultimement périodique. Notons R sa période et h le rang d'entrée, on a donc $\forall r \geqslant h\ \check{t}_{r+R} = \check{t}_r$.

Si $\overline{c_l c_{l-1} \ldots c_0}$ est l'écriture d'un entier naturel n en base b, on a $\prod_{i=0}^{h-1} \check{t}(i, c_i) = t_{n - b^h [\frac{n}{b^h}]}$ et

$$t_{b^h [\frac{n}{b^h}]} = \prod_{i=h}^{l} \check{t}(i,c_i) = \prod_{I=0}^{[\frac{l-h-1}{R}]} \prod_{i=0}^{R-1} \check{t}(h+i+IR, c_{h+i+IR}) = \prod_{I=0}^{[\frac{l-h-1}{R}]} \prod_{i=0}^{R-1} \check{t}(h+i, c_{h+i+IR})$$

On a (3.1) si on pose $\bar{t}_N = t_{b^h N}$, et l'identité ci-dessus montre que la suite $\bar{t}$ est bien b^R-multiplicative et vérifie la condition de finitude. □

Bibliographie

[1] J.-P. Allouche, J.Shallit, The Ubiquitous Prouhet-Thue-Morse sequence, *Sequences and their applications (Singapore)*, 1998, 1–16.

[2] J.-P. Allouche, J.Shallit, *Automatic sequences*, Cambridge University Press (2003).

[3] A.T. Benjamin, J.J. Quinn, The Fibonacci Numbers – Exposed More Discretely, *Mathematics Magazine* vol **76** no3 (June 2003), 182–192.

[4] Z.I. Borevitch et I.R. Shafarevitch, *Théorie des nombres*, Gautier-Villars Paris (1967).

[5] O.Carton, *Langages Formels, Calculabilité et Complexité*, Vuibert (2008).

[6] J. Coquet, A summation formula related to the binary digits, *Inv. Math.* **73** (1983), 123–137.

[7] C. Dartyge and G.Tenenbaum, Sommes des chiffes de multiples d'entiers, *Ann. Inst. Fourier (Grenoble)* **55** (2005), no.7, 2423–2474.

[8] F.M. Dekking, 0n the distribution of digits in arithmetic sequences, *Séminaire de théorie des nombres de Bordeaux* (1982-1983), exp.32.

[9] H.G. Diamond and H. Pollard, *The theory of algebraic numbers 2nd edition* , The Mathematical Association of America (1975).

[10] M. Drmota, C. Mauduit and J. Rivat, The sum-of-digits function of polynomial sequences, *J. Lond. Math. Soc. (2)* **84** (2011), no.1, 81–102.

[11] M. Drmota and J.Morgenbesser, Generalized Thue-Morse sequence of Squares, *Israel J. Math.* **190** (2012), 157–193.

[12] M. Drmota and M. Skałba, Sign-changes of the Thue-Morse fractal function and Dirichlet L-series, *Manuscripta Math.* **86** (1995), no.4, 519–541.

[13] M. Drmota and M. Skałba, Rarified sums of the Thue-Morse sequence, *Trans. Amer. Math. Soc.* **352** (1999), 609–640.

[14] M. Drmota and Th. Stoll, Newman's phenomenon for generalized Thue-Morse sequences, *Discrete Math.* **308** (2008) no.7, 1191–1208.

[15] J.-M. Dumont, Discrépance des progressions arithmétiques dans la suite de Morse, *C. R. Acad. Sc. Paris Sér I Math.* **297** (1983), no.3, 145–148.

[16] K.J. Falconer, The Hausdorff Dimension of Some Fractals and Attractors of Overlapping Construction, *Journal of Statistical Physics* Vol. **47**, Nos.1/2 (1987), 123–132.

[17] J.-P. Gazeau and J.-L. Verger-Gaugry, On the spectrum of the Thue-Morse quasicrystal and the rarefaction phenomenon, *J. Théor. Nombres Bordeaux* **20** (2008), 673–705.

[18] A.O.Gelfond, Sur les nombres qui ont des propriétés additives et multiplicatives données, *Acta Arith.*, **13** (1968), 259–265.

[19] S. Goldstein, K. Kelly and E. Speer, The Fractal Structure of Rarefied Sums of the Thue-Morse Sequence, *J. Number Theory* **42** (1992), 1–19.

[20] P.J. Grabner, A note on the parity of the sum-of-digits function, *Actes 30ième Séminaire Lotharingien de Combinatoire (Gerolfingen,1993)*, 35–42.

[21] A.Hof, On Diffraction by Aperiodic Structures, *Commun. Math. Phys.*, **169** (1995), 25–43.

[22] R. Hofer, Coquet-type formulas for the rarefied weighted Thue-Morse sequence, *Discrete Mathematics*, **311** (2011), 1724–1734.

[23] D.Knuth, *The art of computer programming, 2d edition*, vol. 2, Addison-Wesley publishing company (1981).

[24] J.P.S. Kung, G.-C. Rota and C.-H. Yan, *Combinatorics : The Rota Way*, Cambridge University Press (2009).

[25] D.W. Matula, Basic digit sets for radix representation of the integers, *Proc. IEEE Symp. Comput. Arith.* **4** (1978), 1–9.

[26] C. Mauduit and J. Rivat, La somme des chiffres des carrés, *Acta Math.* **203** (2009), 107–148.

[27] H.M. Morse, Recurrent geodesics on a surface of negative curvature, *Trans. Amer. Math. Soc.* **22** (1921), 84–100.

[28] D.J. Newman, On the number of binary digits in a mutiple of three, *Proc. Amer. Math. Soc.* **21** (1969), 719–721.

[29] E. Prouhet, Mémoire sur quelques relations entre puissances des nombres, *C.R. Acad. Sci. Paris Sér I* **33** (1851), 225.

[30] G.-C. Rota, On the Foundations of Combinatorial Theory I. Theory of Möbius Functions, *Z. Wahrscheinlichkeitstheorie* **2** (1964), 340–368.

[31] V.S. Shevelev, On the number of solutions of the congruence $\sum_{i=1}^{s} x_i \equiv r \bmod k$, *Izv. Vyssh. Uch. Zav., Sev.-Kavk. reg.*,**2**, 25–37 (1996).

[32] V.Shevelev, Generalized Newman Phenomena and Digit Conjectures on Primes, *Int. J. Math. Sci.*, 2008.

[33] R.P. Stanley, *Enumerative combinatorics*, Cambridge University Press (1997).

[34] G. Tenenbaum, Sur la non-dérivabilité de fonctions périodiques associées à certanes formules sommatoires, *The mathematics of Paul Erdös, I* 117–128, *Algorithms Combin.* **13** (1997).

[35] A.Thue, Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen, *Norske vid. Selsk. Skr. Mat. Nat. Kl.* **1** (1912), 1–67. Recopié dans "Selected mathematical papers of Axel Thue," T.Nagell, ed., Universitetsforlaget, Oslo, 1977, pp.413–478.

[36] J.R. Trollope, An explicit expression for binary digital sums, *Math. Mag.* **41** (1968), 21–25.